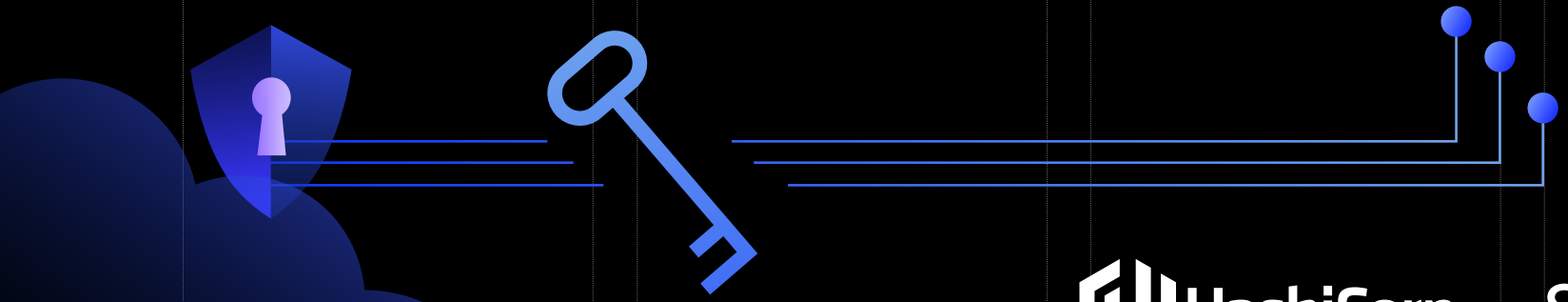
Case Study

SOFTSERVE USES HASHICORP VAULT TO KEEP CLIENT SECRETS SAFE

SoftServe chooses HashiCorp Vault tool to keep a client's platform secrets secure and accessible to users



HashiCorp softserve

OVERVIEW

You know that keeping secrets secret on your platform is crucial. Secret information can be anything that requires restricted access: customer data, pricing information, sales plans, passwords, and the list goes on. And the most important thing about secrets is they must be accessible to those who need to see them, and not to those who shouldn't.

Secret handling is now required everywhere. That means secure, sensitive information with granular access control, system compliance with industry regulations, and a secure way to make your system less vulnerable and more stable in the face of potentially dangerous activities.

And not just in fancy, newly built applications, but with ubiquitous tools such as a system monitoring system. You can't get away with using static passwords and keys anymore.

It's essential to ensure that your platform's security measures are up to date and cutting edge. Migration from older, less capable software is always a major undertaking. When this happens, you need a firm set of cybersecurity goals and tools at the center of your implementation plan.

Our client, a global provider of high-tech expertise and solutions to governments, businesses, and nonprofit organizations realized their growth required the migration of their present monitoring system to a more powerful solution.

CHALLENGES

As part of this migration, our client identified several challenges:

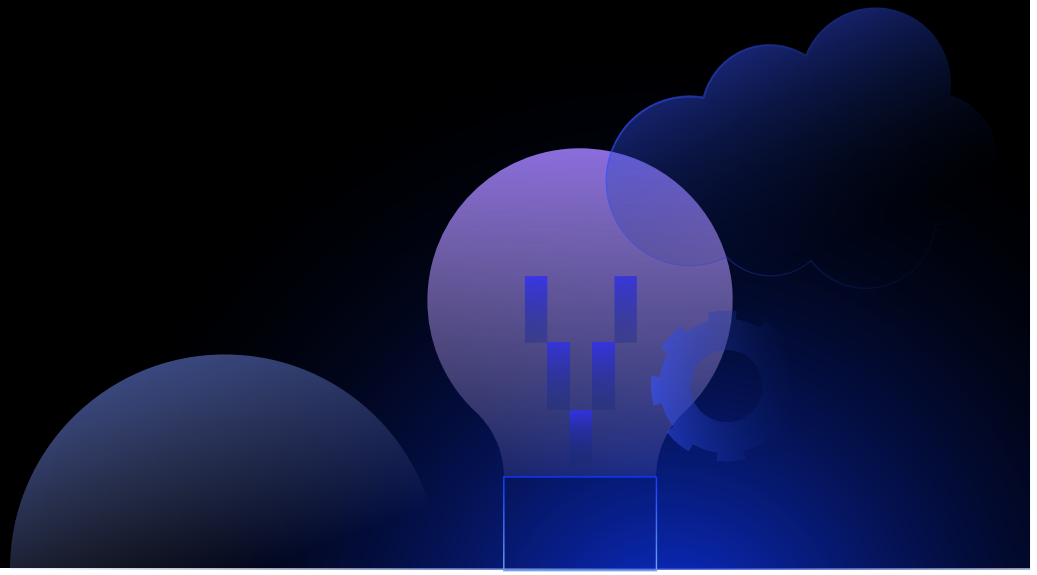
- The need to protect secrets by monitoring their system from potential security threats, which would ensure granular, role-based access where only authorized users have access
- A reliable and highly available solution to host secrets
- Round-the-clock platform monitoring, which would allow for a highly available monitoring system

The client also desired other features, including:

- Proven cybersecurity
- A modern platform with a long support cycle
- Flexibility and extensibility
- The ability to perform self-diagnostic and auto remediation

As they continued their preliminary research into the project, they recognized the scope of the migration would require the help of a reliable technology partner that had extensive expertise within the cybersecurity domain and in planning and executing complex projects with distributed product development teams using the current best practices. SoftServe got the nod.

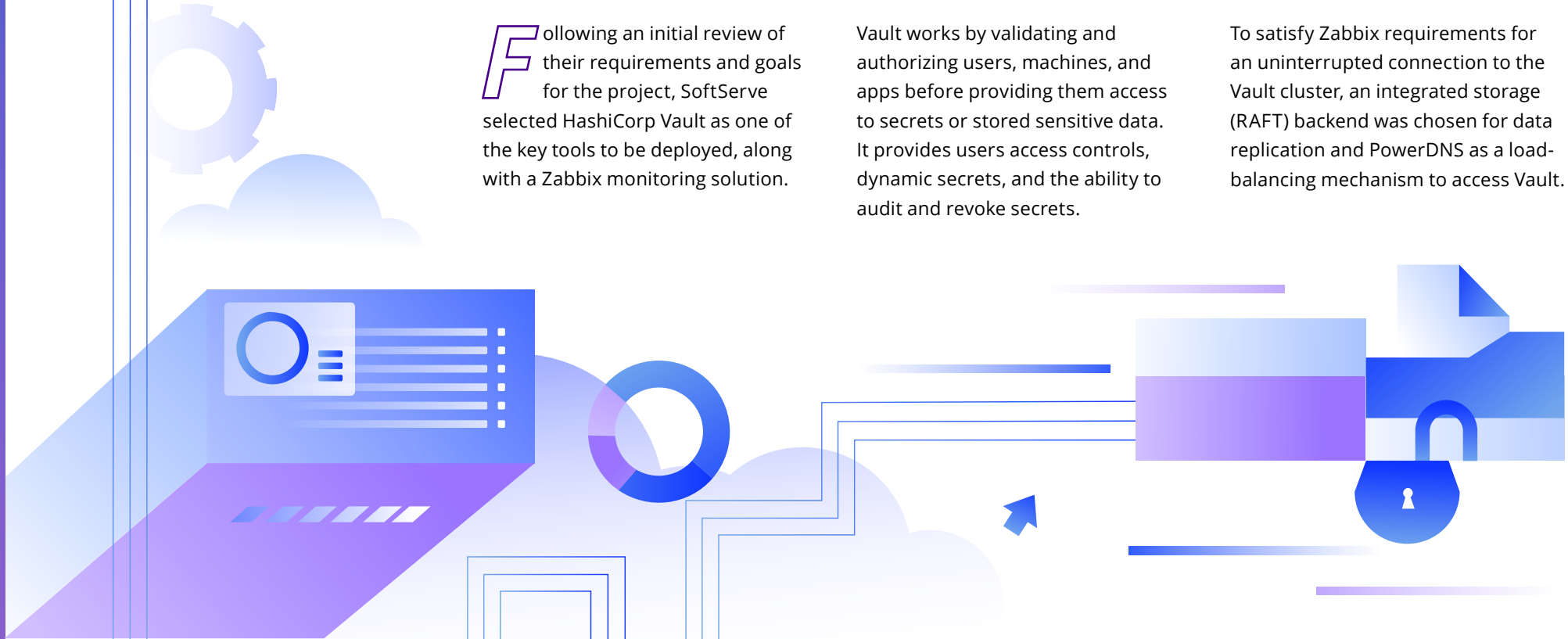
SOLUTION



Following an initial review of their requirements and goals for the project, SoftServe selected HashiCorp Vault as one of the key tools to be deployed, along with a Zabbix monitoring solution.

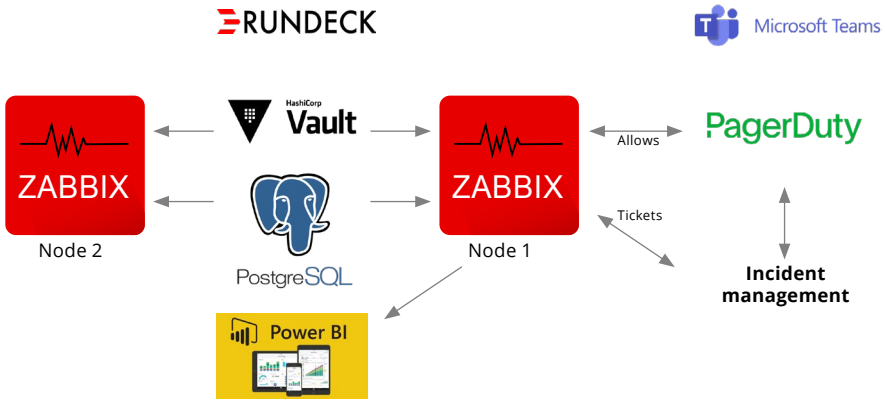
Vault works by validating and authorizing users, machines, and apps before providing them access to secrets or stored sensitive data. It provides users access controls, dynamic secrets, and the ability to audit and revoke secrets.

To satisfy Zabbix requirements for an uninterrupted connection to the Vault cluster, an integrated storage (RAFT) backend was chosen for data replication and PowerDNS as a load-balancing mechanism to access Vault.



PLANNING AND PROJECT IMPLEMENTATION

In planning this project, a dedicated team from SoftServe was formed with members of our client's DevOps team to determine their requirements.



SoftServe designed, configured, and implemented a new monitoring system, along with PowerDNS and HashiCorp Vault to satisfy the high availability option. Our solution allowed our client to monitor several parameters within a network, including the health and integrity of associated servers.

THE TECH STACK

ZABBIX

POSTGRESQL

HASHICORP VAULT

POWERDNS

RESULTS

As a result, SoftServe was able to develop a reliable monitoring solution with secure methods for storing secrets and other sensitive information, along with the automated provisioning of customer services to the Zabbix monitoring system. That allowed our client's DevOps teams to onboard services to the Zabbix monitoring system and create a pre-defined secret engine within HashiCorp Vault.

Overall, HashiCorp Vault can protect you from leaked credentials that can damage your organization's business and reputation by configuring your generated secrets to expire — or be maintained — for as long as you desire.

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.

Hot Links

info@softserveinc.com
www.softserveinc.com

Contacts

NORTH AMERICAN HQ

201 W 5th Street, Suite 1550
Austin, TX 78701
USA +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