Using Vault to Protect a Leading Software Company's Secrets and User Data Across Clouds and Datacenters

This company builds popular software and digital experiences used by millions of people worldwide. Whether working in the creative world, watching movies and tv shows, or streaming the big game on your phone, you've probably used their software.

CUSTOMER STORY

HashiCorp

800 million

Vault transactions per month

30,000+

secrets saved from maintaining custom secrets management solutions

100+

employee hours saved annually with automatic secret rotation

150,000

applications and hosts managed with Vault

Securing secrets and application data is a complex task for globally distributed organizations.

One small mistake can lead to a major breach. Managing secrets for over 60 products across 150,000 hosts and four regions requires a different approach altogether. The company sought to reduce the risk of secret sprawl and data exposure by centralizing and tightly controlling access to secrets and securing data across clouds, applications, and systems based on trusted identities with Vault. By introducing HashiCorp Vault as a single security solution, the company not only improved organizational efficiency and reduced risk of secret sprawl, it reduced costs and overhead associated with managing and supporting different security solutions.

Today, the company is running Vault globally supporting over 800 million monthly transactions. Since the initial proof of concept and rollout, the company has grown Vault adoption 600%, saving the company hundreds of employees hours spent managing thousands of secrets and greatly reducing the operational burden around issuing secrets throughout the company.

Vault as a Service

The company runs Vault as a centralized secrets management and application data encryption solution by leveraging the identity of thousands of users and hundreds of thousands of the company's systems and applications. Vault is a geographically distributed solution for teams to manage and secure access to organizational secrets and secure data. Vault is deployed across their fleet of different clouds and data centers, including AWS, Azure, and private data centers. The company runs 14 Vault Enterprise clusters that replicate secrets, access, and encrypt data and process over 800 million transactions every month, and billions annually. Vault has dramatically decreased the average time to process secrets distribution across 10,000 hosts from over 4 minutes to under one second.

Introducing Vault has significantly reduced organizational costs and overhead for the company by consolidating the management and support of disparate solutions into a single solution. Licensing, hardware, and support costs around maintaining different solutions for different teams and environments have been reduced. Teams and engineers building different internal solutions are now able to focus on other projects, saving the company a significant amount of operational costs tied to secrets management. Additionally, with Vault's RESTful API, engineering and product teams have been able to easily onboard and adopt Vault with little or no downtime, regardless of their identity platforms or if applications are legacy or live in different environments -- this introduced a single endpoint to handle secrets access and requests, as well as standardizing data encryption.

Before Vault, engineers at the company spent hundreds of hours manually performing secrets rotation across their entire infrastructure (thousands of hosts, etc). Now, they get all that time back since the operational burden is eliminated with Vault's dynamic secrets and the ability to programmatically and dynamically roll, renew, and rotate secrets across their global infrastructure. Furthermore, bringing these operations and managing access to secrets through Vault, the company maintains and programmatically ensures auditing, compliance, and governance through global policies and audit logging.

Moving from Multiple Secrets Management Solutions to Consolidating on Vault

In late 2016, the company looked at HashiCorp Vault as a possible pilot solution to tackle their growing need to centralize their secrets management through a single workflow. The company lacked a company-wide solution for maintaining and managing secrets. Without a global solution, they were unable to audit secret access across all teams and infrastructure. This created a sprawl of secrets and secret management systems. Or worse, there were no secrets management solutions in place for some teams.

This company has been around for over 30 years and has three large platforms around their creative, document, and marketing and analytics suites. The move to cloud led the company to build and integrate numerous solutions to solve secrets management and data encryption. However, they needed to find one solution that would scale with the company and their growing portfolio of products and frequent acquisitions. Additionally, the company's move from legacy applications to microservices in multiple clouds and globally distributed data centers needed a solution that truly supported hybrid infrastructure along with large-scale geographic distribution and throughput.

Conclusion

Today, the company's teams and products use Vault as a global solution for managing billions of secrets and access requests across the globe. Over the course of adoption, the company worked to remove bottlenecks and improve efficiency by automating secrets and policy management while reducing complexity and costs around managing different secret solutions. As the company's product teams and infrastructure grow, Vault's extensibility ensures that adding different technologies, environments, and sources of identities integrate seamlessly to allow for fast adoption and increased productivity.


HashiCorp