



YAHOO!
JAPAN

CUSTOMER STORY

Secrets at scale for Japan's most visited website

The popular website that offers search, news, e-commerce, and many more services uses HashiCorp Vault to secure credentials and keys across its entire cloud-based environment.

// Infrastructure Enables Innovation

About Yahoo! JAPAN

Launched on April 1, 1996 by Yahoo! JAPAN Corporation (headquarters: Chiyoda-ku, Tokyo; CEO: Kentaro Kawabe), a subsidiary of Z Holdings Corporation, Yahoo! JAPAN is now one of the largest online comprehensive information websites in Japan and offers nearly 100 services, including search, news, and e-commerce. It has approximately 80 million users.

FAST FACTS



Most visited site in Japan



Eliminated unplanned application and service downtime



Drastic improvements in security posture



Approximately 7,000 employees



Reduced risk of breach due to encryption key exposure



Accelerated time to market via automated key management

“ Vault supports a variety of authentication patterns and provides support for flexible encryption key usage, making it easier to scale even with frequently changing application environments and creates a more cost effective way to manage an increasing number of secrets and keys. ”

Better secrets to serve the masses

Japan has long been a hotbed of technical innovation and leadership and Yahoo! JAPAN is one of the country's most highly regarded IT examples. Yahoo! JAPAN has grown to become the most visited website in the country, with approximately 80 million users.

Securely and reliably processing extremely large volumes of web visits, data queries, and myriad data-related services requires an expansive IT infrastructure. Since the infrastructure has numerous network segments and connected services with sensitive information, it needs to be protected securely. That requires a comprehensive key management system capable of handling both a large number of key requests and everyday management.

“We built out our own private cloud environment to increase our business agility and accelerate service development to keep up with the changing demands of the market and our customers,” says Kento Matsui, manager of the data protection technology in Yahoo! JAPAN's Security Technology Department. “While a cloud-native architecture is a necessity in today's business climate, the growing number of stateless applications in that environment created new challenges around how to reliably handle issuing and managing such a large number of encryption keys. That compelled us to rethink our approach to secrets management and security.”

Securing secrets across platforms and datacenters

Yahoo! JAPAN earned its market-leading position by offering users of a wide array of web services. From search capabilities and email to local news feeds and business services, each of the company's services are supported by both development teams of the service itself and infrastructure teams which provide infrastructure and platforms for the services.

Those systems and services must be connected via a robust process for handling encryption keys and credentials to help ensure that only authorized users and destination systems can access areas housing mission-critical information or sensitive data. Matsui says that as a high-volume, web-based business it's imperative that every backend system work at peak efficiency to support its everyday users and be able to absorb huge spikes in traffic volume.

"Our previous secrets management tool simply cached keys on the application side to keep them available in the event of an interruption," he explains. "Along with the wider use of our cloud environment and the growing number of applications, the number of requests compared to the previous environment is expected to increase drastically. This poses the risk of overloading the key management system to the point of failure and having an immediate negative impact on our customers. We needed a way to maintain the safety of the key management system, while at the same time raising availability and performance across the board."

Challenges



Securely managing credentials and access keys over multiple datacenters



Ability to deliver required performance while ensuring the safety of the key management system



Creating a way to achieve high availability so as to maintain high system reliability, as well as providing high maintainability

Ensuring encryption key confidentiality and availability quickly

Matsui is a professional who has gained extensive experience in cybersecurity and ID authentication solutions as the leader of a development team. For the development and operation of a next-generation key management system, his team had also begun searching for a system that can deliver both security and performance.

The Yahoo! JAPAN team initially considered developing a new encryption key management solution independently. Doing this, however, posed a challenge since managing all the internal encryption keys requires the time-consuming task of ensuring absolute system reliability. The team realized that if it were to carry out testing and verification — to confirm that there is no problem with the encryption implementation, the secrecy of the encryption keys is sufficiently maintained, and availability to withstand large-scale failures can be ensured — it would need at least six months, resulting in a longer lead time to deliver a new encryption key management solution.

Instead, they sought a third-party solution capable of supporting access control across the company's geographically distributed datacenters and cloud availability zones. The new solution also had to be resilient, capable of replicating clusters and coordinating with Hardware Security Modules (HSMs) — modules that physically protect encryption keys and signatures — to ensure maximum availability.

Yahoo! JAPAN chose HashiCorp Vault to give their development and infrastructure teams a secure, easy-to-use encryption key management solution. Vault's adoption record and high reliability were also important points for selection. With Vault, the company can manage various encryption keys such as signature key, signature verification key, API token and DB authentication information required for service development.

“By adopting Vault,” says Matsui, “we were able to develop a high-availability system that incorporates the latest cryptographic technologies that Vault offers, while maintaining the functionality of our existing key management system. In light of it being able to deliver the availability that we need while ensuring safety, we consider Vault to be the right choice.”

Less downtime, faster delivery, and happier customers

Deploying HashiCorp Vault has significantly improved the performance, availability, and reliability of Yahoo! JAPAN's key management system, helping to accelerate the otherwise time and resource-intensive process of securely managing credentials and access keys across its sprawling cloud environment.

With Vault, Yahoo! JAPAN avoided at least half a year's worth of development that they would have had to invest if the team had tried to build its own key management solution. While specific improvements in cost management, incident prevention, and time-to-market are complicated to calculate, Matsui contends that Vault has made a substantial contribution to improving his team's operations overall.

"An encryption key has to have either cryptographic protection or physical protection, or both," he states. "It's not easy to achieve both cryptographic and physical protections while also maintaining very steady performance. Vault supports HSM and provides cryptographic protection on the basis of physical protection. Even though performance is usually sacrificed for physical protection, using Vault enabled us to solve the challenges and achieve both. This made it possible for us to deliver safer services to our users and create the added value of a shortened development period."

Matsui also appreciates the opportunity he had to talk with a Vault Enterprise Architect through HashiCorp's support team. A workshop was held to discuss system configuration risks with the architect team and prioritize risk countermeasures based on clear ratings, which Matsui contends served as a major inspiration during the adoption process, helped identify areas for improvement and optimization, and provided an opportunity to work to deliver better services speedily.

Outcomes



Achieved substantially higher safety and functionality than the previous key management system



Developed and delivered a system significantly quicker

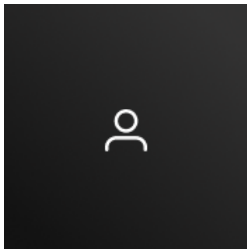


Achieved a more robust configuration by assessing security risks through a workshop with a HashiCorp architect

Solution

Yahoo! JAPAN uses HashiCorp Vault to protect essential authentication information and encryption keys across multiple geographically dispersed locations, private cloud platforms, and dozens of web-based services.

Yahoo! JAPAN Partners



Mr. Kento Matsui joined Yahoo! JAPAN directly out of college and is the manager of data protection technology.

Kento Matsui, Manager of the Data Protection Technology, Security Technology Department, Yahoo! JAPAN

