HashiCorp

UBISOFT | CUSTOMER STORY

Game time

The pioneer in online gaming uses HashiCorp Vault to enhance security, availability, and performance across a global gaming platform.

// Infrastructure Enables Innovation

Summary

Founded in 1986, Paris-based Ubisoft's 20,000 global team members, working across more than 30 locations around the world, are bound by a common mission to enrich players' lives with original and memorable gaming experiences. The company is the publisher of many acclaimed video game franchises such as Assassin's Creed, Rainbow Six, Far Cry, Watch Dogs, Rayman, and Just Dance.

FAST FACTS

141 million unique players in FY21 over consoles and PC

Highly distributed across 7 regions

Reduced risk of breach due to secrets exposure

500+ active entities accessing Vault secrets per day

1000s of applications

Improved security posture by adopting secrets management best practices

> HashiCorp Vault had all the features, functionality, and security settings we needed to drive greater standardization and adoption across the company while still maintaining each team's autonomy and unique work style."

DONALD HAVAS,
ASSOCIATE DIRECTOR, UBISOFT

Gaming goes global

For nearly 40 years, Ubisoft has been at the forefront of video game development, designing and publishing some of the best-known game franchises in history.

As video games evolved from single platform CD-based assets to more immersive, visually engaging experiences delivered online, the supporting IT infrastructure required to keep games operating at peak performance has also evolved. For Ubisoft, that meant running as many as half a dozen of its own data centers to deliver the best online experience. Starting with bare metal servers, then a virtualized environment and an OpenStack private cloud, the company's expansive IT footprint now has since been deployed as a platform as a service (PaaS) across several regions, with thousands of applications alongside workloads across multiple public cloud providers. This amount of growth on a dispersed and heterogeneous infrastructure also brought its own secrets management challenges and potential secret sprawl.

"We've always preferred to treat our individual teams as studios and allow them to work autonomously because it makes them more agile and responsive to customer demands and the needs of the market without having to rely on a central engineering team to lead the way," explains Donald Havas, associate director at Ubisoft. "But it also creates some unique and concerning challenges when teams have their own approaches to managing secrets and security because it can result in limited visibility, and a lack of resilience that invites service interruptions or degradation."

Standardized secrets for non-standard development

In the past, individual Ubisoft teams had managed their own secrets and tokens — governing access to everything from MongoDB or other databases to API keys, software development kits (SDKs), and its Kubernetes-powered CI/CD pipeline. With this fragmented approach, teams managed their secrets using a mix of internal and third-party tools, such as Centrify and Passwork, resulting in few best practices and limited operational transparency.

In a market in which game developers are judged not just by the quality of the game design and gameplay but also by their availability, performance, and security, leaving secrets management up to the individual groups seemed destined to create unnecessary issues for developers and the brand at large.

"We had some incidents in the past where the secrets expired and we didn't have visibility or the ability to track them down, which resulted in some unplanned downtime," says Shuichi Sekino, head of product for Ubisoft's IT - Engineering and Platform team. "Even a one-day outage due to a certificate expiring or someone changing a password to a certain site can significantly impact the gaming experience, whether that's registering a new player or playing a game itself."

Havas says that Ubisoft's IT and security teams began creating a proof of concept around standardizing and automating their secrets management to promote resilience, availability, and security without interfering with the studio teams' game development progress. "HashiCorp Vault had all the features, functionality, and security settings we needed to drive greater standardization and adoption across the company while still maintaining each team's autonomy and unique work style," he says. Some of the use cases these teams have prioritized include support for different secret types, user interface, application programming interface (API), role based access control (RBAC), logging and auditing, and metadata.

The open source version of Vault aligns well with Ubisoft's historical preference for customizable open source technologies. More importantly, the tool's rich automation capabilities and agnostic posture enables Ubisoft to manage secrets at scale and across virtually any environment or platform.

"Our games' matchmaking might be in Azure, telemetry could be in AWS, and other functions might run on Google in this complex ecosystem. Manually managing secrets and rotating credentials across all those platforms to keep them secure and operational manually is literally impossible," Havas explains. "Vault automatically rotates access to tokens, passwords, certificates, and encryption keys the same way across every public and private cloud so our developers don't have to waste time doing it themselves."

Challenges

Standardizing secrets management best practices without impacting individual studio workflows

Reducing the risk of data breach or unplanned service unavailability and performance degradation

Replacing manual secrets and token management with automated solutions

> Vault doesn't require a long learning curve or special training to get it up and running, so we were able to begin centralizing our secrets management operations and applying best practices across all our teams almost instantly with significantly fewer resources to manage the tool."

SHUICHI SEKINO,
HEAD OF PRODUCT, UBISOFT

Greater availability, lower risk, and an exceptional gaming experience

Despite other solutions also offering some automation features, none matched Vault's multi-platform interoperability and intuitive user interface. Vault was an ideal solution to accommodate Ubisoft's needs.

"Vault doesn't require a long learning curve or special training to get it up and running, so we were able to begin centralizing our secrets management operations and applying best practices across all our teams almost instantly with significantly fewer resources to manage the tool," Sekino says. "The teams who hadn't been using Vault the right way or hadn't been using it at all can now automatically issue, retire, or rotate secrets for their entire studio to greatly reduce the risk of a breach or misconfiguration taking key parts of the game offline for even a few minutes."

Havas says that adopting Vault open source and Vault Enterprise — in addition to the company's extensive use of HashiCorp Terraform to provision the necessary infrastructure to run its various services — is essential to helping maintain the quality, performance, and upgraded gaming experience its global users have come to expect.

"The HashiCorp solutions have helped us dramatically improve our quality of service and push our service level objectives well beyond industry standards by virtually eliminating disruptions and delays frequently caused by manual secrets management and infrastructure orchestration," he says. "With that all settled, we have the confidence to explore ways of expanding our platform with things like API gateways and a service mesh that will help us continue to set the standard for online gaming experiences for generations to come."

Outcomes

Pushed service level objectives to three 9s (99.9% uptime), in excess of industry standards

Enabled automatic secrets rotation across multiple cloud platforms and reduced costs associated with manual management of secrets

Eliminated unplanned service interruptions caused by expired certificates or misconfigured secrets

Solution

Ubisoft uses HashiCorp Vault to automatically assign, retire, and rotate secrets across various systems and services that reside in multiple public and private clouds around the world.

Ubisoft Partners

Donald Havas is the associate director at Ubisoft, responsible for building the technological ecosystem and global infrastructure needed to propel the company into the future of gaming. Prior to joining Ubisoft, Donald spent nearly two decades serving in various software development and production management roles at well-known companies like Amazon Web Services and Convergys.

Donald Havas,
Associate Director. Ubisoft

Shuichi Sekino is the head of product for IT - Engineering and Platform at Ubisoft, and leads the product organization for this team. The team builds cloud-native solutions that simplify the experience of developing, deploying, and scaling applications used by game teams such as Far Cry, Rainbow Six, and Assassin's Creed. The product organization includes product management, UX design, technical documentation, and developer relations.

Shuichi Sekino,
Head of Product, Ubisoft

Technology Stack

- Infrastructure: AWS, Google Cloud, Azure, OpenStack on-premises
- Workload type: Game servers, backend services, databases
- Container Runtime: Docker
- Orchestrator: Kubernetes, Rancher
- CI/CD: GitLab, Jenkins
- Version Control: GitLab, Perforce
- Provisioning: HashiCorp Terraform, Red Hat Ansible
- Security management: HashiCorp Vault, Azure Active Directory


HashiCorp