

A CASE STUDY

## How an Organization with a Tech Skills Gap Improved their Security Posture with the RPT Accelerator

A case study on how RPT helped an Ivy League university launch HashiCorp Vault & Kubernetes in a private cloud environment.

© 2024 by River Point Technology. All rights reserved.



## **EXECUTIVE SUMMARY**

In today's rapidly evolving business environment where enterprises rely on the cloud, maintaining a strong security posture is paramount. But it can also be a major challenge, if like many organizations your tech team lacks the time or skill set to focus on critical security initiatives.

That's where our client, an iconic lvy League university, found themselves. Responsible for safeguarding the information of hundreds of thousands of students, alumni, and staff along with vital research, their team was overwhelmed. From ensuring the protection of critical systems, safeguarding data, adeptly managing secrets, to addressing governance compliance; modernizing the security of their organization's cloud infrastructure and overall tech stack would be a big undertaking to navigate and manage on an on-going basis.

It's a common experience for technologists, administrators, CIOs, and CTOs to find their teams lacking the necessary time and expertise to fully dedicate to such significant initiatives. With their attention consumed by day-to-day operations, they often require a capable guide to step in and assume leadership in tackling their secrets management and infrastructure security initiatives.

That's where the award-winning team at River Point Technology (RPT) came in. The RPT Accelerator, an annual subscription offering, ensured that the Ivy League university's tech team had a trusted partner to turn to all year long as they deployed HashiCorp Vault and Kubernetes within a private cloud environment. From Day 0 to Day 1 and onto Day 2, the experts at RPT were there to manage all the complexities associated with improving the organization's security posture and to ensure that everything continues to run smoothly. They "love having a guide every step of the way" and can rest a little easier at night knowing the industry's best have their backs.

#### **Primary Business Objective**

- Partner with a firm that's an expert on cloud and infrastructure security who can fill a critical skills gap reliably on an annual basis.
- Understand & use best practices for deployment of HashiCorp Vault.
- Unite Kubernetes with HashiCorp Vault and traditional applications within a private cloud infrastructure.

#### **Secondary Objectives**

- Obtain in the moment support for immediate challenges
- Accelerate adoption & Day 2 operations
- Augment business model and create supplementary revenue streams



## THE SOLUTION

#### **RPT's Accelerator**

The RPT Accelerator, grounded in Value Creation Technology, drives continuous improvement in cloud and DevOps technology. Through standard and personalized education and training on our private platform, teams stay current and gain insights. Scheduled "office hours" address Day 2 challenges, while "advisory hours" provide personalized advice on advanced issues. Utilizing our proprietary portal streamlines communication and sharing. Quarterly reviews with key stakeholders ensure ongoing progress and maximum value from technology investments.

#### Automated Deployment of Vault Clusters

The deployment of Vault clusters is a critical task for any organization that uses Vault to manage its secrets. A well-deployed Vault cluster is highly available and redundant, and it can be easily upgraded to new versions.

RPT's Accelerator guided the automated deployment of Vault clusters using the Vault Helm chart. The Vault Helm chart simplifies the deployment of Vault on Kubernetes and provides a number of features that make it ideal for automated deployments, including:

- The ability to customize configurations while maintaining consistency across environments
- The ability to deploy Vault using a single configuration option
- The use of StatefulSets, pod affinities, and a highly available storage backend (Raft) to ensure that Vault is highly available and redundant
- The ability to roll out new versions of the Vault Helm chart and Vault pods seamlessly
- Used the Vault Agent Injector, CSI Provider, and the Vault Operator to natively integrate Kubernetes applications with Vault without them needing to be "Vault aware".

#### **Technical Goals**

- Accelerate the adoption of secure secrets management.
- Using HashiCorp Vault as a secrets manager for traditional & non-traditional applications
- Integrate Kubernetes with HashiCorp Vault and traditional applications on a private cloud
- Integrate with the CI/CD platform that provisions workloads to VMware environments.
- Define dynamic secrets for Kubernetes and demonstrate how to use the Vault operator for static and dynamic secrets.
- Validate and Harden Secrets Manager infrastructure
- Showcase new addition to repo for creating a database application using dynamic secrets.



#### **Benefits of Automated Deployment of Vault Clusters**

There are a number of benefits to automating the deployment of Vault clusters, including:

**Reduced risk of human error:** Automating the deployment process can help to reduce the risk of human error. This is because the deployment process is defined in code, which can be easily reviewed and tested.

**Improved consistency of deployments:** Automating the deployment process can help to improve the consistency of deployments. This is because the deployment process is the same for every environment, which can help to avoid configuration errors.

**Easier to upgrade Vault to new versions:** Automating the deployment process can make it easier to upgrade Vault to new versions. This is because the upgrade process can be automated, which can save time and effort.

**Native integration with Kubernetes applications:** By using the Vault Agent Injector, CSI Provider, or the Vault Operator, Kubernetes applications can natively integrate with Vault without them needing to be "Vault aware". This can make it easier to manage secrets in Kubernetes applications.

#### Why HashiCorp Stack?

HashiCorp Vault excels in managing sensitive information such as API keys, passwords, and encryption keys. Using it with Kubernetes ensures secure storage and dynamic handling of secrets, crucial for protecting sensitive data across various applications. For an university handling diverse applications, maintaining consistent security policies is vital.



Vault allows defining and enforcing policies centrally, ensuring a uniform security posture across both traditional and non-traditional applications. Leveraging Vault with Kubernetes allows seamless integration with the orchestration platform. This integration enables automated secret retrieval, making it easier to manage secrets in a dynamic and scalable containerized environment.

River Point Technology's Accelerator successfully guided the school's team through HashiCorp's suite of products to elevate the security of secrets management, bringing both enhanced protection and ease to their DevOps team. By implementing HashiCorp's solutions, we helped fortify the infrastructure's secrets with advanced encryption and dynamic management capabilities, ensuring a robust defense against potential security threats.



## **TOP 10 CHALLENGES OF INTEGRATING KUBERNETES WITH HASHICORP VAULT**

The journey of integrating Kubernetes (K8s) with HashiCorp Vault and traditional applications on a private cloud can be a complex undertaking. That's why organization's like this Ivy League university turn to RPT. Below we highlight the top 10 challenges a team may face when integrating Vault and K8s.

- **1 Authentication and Authorization:** Configuring proper authentication and authorization mechanisms to control access to Vault secrets for both Kubernetes and traditional applications can be challenging.
- **2 Secrets Management:** Managing secrets across different platforms, ensuring their security, and automating their lifecycle is a fundamental challenge.
- **3** Secret Rotation: Implementing automated secret rotation policies and procedures for secrets stored in Vault can be complex, especially for legacy applications that may not support dynamic secret retrieval.
- 4 **Networking and Security:** Establishing secure communication between Kubernetes pods, traditional applications, and Vault while maintaining network segmentation and firewall rules can be tricky.
- **5** Integration Complexity: Integrating Vault with a variety of application types, databases, and cloud services, especially when dealing with legacy systems, can lead to integration complexities.
- **6 Compliance and Auditing:** Meeting compliance requirements and tracking access and usage of secrets for auditing purposes can be challenging, especially in regulated industries.
- **7** Secrets Versioning: Managing different versions of secrets, ensuring backward compatibility, and handling secrets rotation gracefully can be complex.
- 8 **Backup and Disaster Recovery:** Developing and testing robust backup and disaster recovery plans for Vault's data and configurations is crucial to ensure business continuity.
- **9** Monitoring and Alerting: Setting up monitoring and alerting solutions to detect and respond to any issues or breaches in real-time is a significant challenge.
- **10 Documentation and Training:** Ensuring that your team has the necessary skills and knowledge to manage and troubleshoot the integrated environment is an ongoing challenge, as technologies evolve.

Addressing these challenges requires careful planning, well-defined processes, and a good understanding of both Kubernetes and Vault, as well as the specific requirements of applications and private cloud environment.



## THE OUTCOME

The RPT Accelerator played a pivotal role in guiding the leveraging of automated pipelines and the Vault Helm chart on clusters. Our process assisted in the build of a container image with the latest Oracle plugin for Vault, ensuring its verification. Utilizing the Vault Helm chart enables flexible customization of configurations while maintaining consistency across diverse environments.

Furthermore, RPT improved deployment efficiency by utilizing a single configuration option, customizing settings for specific resources. The use of StatefulSets, pod affinities, and a resilient Raft-based storage backend guarantees the high availability and redundancy of Vault. Upgrades are seamlessly conducted through the deployment of new chart versions, enabling smooth, rolling updates of Vault pods.

#### **Technical Outcomes & Deliverables**

- Deployment of Vault clusters managed by pipelines and automated through the use of the Vault Helm chart to OpenShift clusters.
- Container image built with the latest version of the Oracle plugin for Vault, and the package is verified.
- Through the use of the Vault Helm chart, configurations can be customized while maintaining consistency across environments.
- With a single configuration option, the deployment is configured to use OpenShift specific resources and settings.
- By using StatefulSets, pod affinities, and a highly available storage backend (Raft), Vault is a highly available, redundant service.
- New versions of the chart can be configured and deployed, and Vault pods are updated in a rolling fashion for seamless upgrades.
- Through the use of the Vault Agent Injector, CSI Provider, or the brand new Vault Operator, Kubernetes applications can natively integrate with Vault without even needing to be "Vault aware.

# **RPT Accelerator®**

With the RPT Accelerator, we are able to validate and harden our Secrets Manager infrastructure following Hashicorp's best practice guidelines. We love having a guide every step of the way. -Senior Infrastructure Engineer



## THE BOTTOM LINE

Facing the challenge of enhancing security without sufficient internal resources, the university leveraged the RPT Accelerator to integrate Kubernetes with HashiCorp Vault and traditional applications on a private cloud. The decision not only bolstered their security posture and upskilled their staff but also enabled the university to facilitate other initiatives. For example, it improved their worldwide online education and certification offerings, enabled monetization of research data, enhanced their engagement with alumni and donors, increased funds received from grants and more.

What seemed like a pure security play clearly delivered so much more value to the organization. That's where RPT's patented Value Creation Technology (VCT) process can help organizations succeed in the cloud. As the university experienced, RPT was able to help them redefine what was really possible with their technology investments. It's a prescriptive approach that accumulated many notable wins.

#### WINS:

**Secured credentials**: The Ivy League college offers a variety of online courses and certification programs to students worldwide. By deploying HashiCorp Vault they can secure student credentials, certificates, and learning progress.

#### Benefits:

- Enhanced Credibility: Students value the security of their digital certificates and credentials. With Vault ensuring the integrity of these documents, the college's certifications gain credibility and are more sought after.
- Secure Digital Badges: The college introduces secure digital badges linked to Vault-protected credentials. Students can showcase their achievements on professional networking platforms, attracting more prospective learners.

**Research data monetization**: The University conducts groundbreaking research across various disciplines. The college offers access to curated research datasets to external researchers, institutions, and companies. Vault ensures secure data sharing while maintaining the integrity and ownership of the data.

#### Benefits:

- Data Licensing: The college offers access to curated research datasets to external researchers, institutions, and companies. Vault ensures secure data sharing while maintaining the integrity and ownership of the data.
- Subscription Models: The introduction of subscription-based access to premium research datasets. Organizations seeking valuable insights are willing to pay for ongoing access, creating a steady revenue stream.
- Data Marketplace: Research data marketplace where academics and researchers can buy and sell datasets securely. A percentage of each transaction contributes to the college's revenue.



#### WINS continued:

Premium Certification Tracks: The college offers premium certification tracks that include enhanced security features powered by Vault. Professionals seeking secure credentials are willing to invest in these premium programs, increasing revenue.

**Targeted Alumni & Donor Engagement**: The college wants to engage alumni and donors in innovative ways. By integrating Kubernetes with Vault they secure personal and financial data for tailored engagement.

Benefits:

- Secure Alumni Profiles: The college secures alumni profiles and engagement data in Vault, ensuring privacy. This enables personalized communication and engagement strategies.
- Exclusive Alumni Services: They offer premium alumni services that provide secure access to career resources, networking events, and educational content. Alumni who value privacy and engagement are more likely to subscribe.
- Donor Data Security: With Vault's robust security, the college builds trust with donors. Donors are more willing to contribute to campaigns and initiatives knowing their data is well-protected.

In these examples, the integration of Kubernetes with HashiCorp Vault and traditional applications on a private cloud enhances the Ivy League college's business model through secure credentials, research data monetization, and targeted alumni and donor engagement. These strategies not only provide valuable services but also attract revenue from students, professionals, researchers, organizations, and donors who prioritize data security and personalized experiences.

#### **Financial Impact: Revenue Generation**

- Cost Savings:
  - Infrastructure Optimization: Kubernetes can optimize resource utilization, reducing infrastructure costs. Allocating resources dynamically as needed, avoiding over-provisioning.
  - Operational Efficiency: Streamlined operations through automation and centralized management of secrets with Vault reduces operational costs.
  - License Management: Efficient management of software licenses lead to cost savings by ensuring they were only pay for what they use.

#### Increased Research Productivity:

- Accelerated research activities due to improved resource allocation and scalability leads to faster research results.
- Productive researchers secure more grant funding and partnerships, indirectly boosting revenue.



#### WINS continued:

- Enhanced Collaboration:
  - Improved collaboration among researchers and with external partners attracts research grants and funding.
  - Collaboration tools and data-sharing capabilities leads to opportunities for joint research projects with external organizations, generating revenue through partnerships.
- Monetization of Research Findings:
  - Securely managing research data in Vault can enable the college to explore opportunities for monetization, such as licensing research findings to industry partners or commercialization.
  - Patents, copyrights, and intellectual property generated from research yields licensing fees and royalties.

#### Improved Reputation:

- An Ivy League college's enhanced reputation attracts more students, research grants, and philanthropic donations, which contributes to financial growth.
- A strong research reputation leads to partnerships with industry and government organizations, which involves financial support or collaborative research projects.

#### Grant Opportunities:

• Successful integration and improved research capabilities make the college more competitive for research grants, leading to additional funding sources.

#### Reduced Downtime and Business Continuity:

• Minimizing downtime and ensuring business continuity through private cloud infrastructure helps prevent financial losses due to disruptions in research activities.

It's clear, the benefits the university has experienced as a result of their engagement with RPT are plenty. They were able to focus on their organizational priorities knowing that a team of experts was there to guide them on the journey. Further, the RPT Accelerator would support their overall goal, assuring deployment aligns with the university's innovative and research-driven ethos, making them a pioneer in leveraging cloud technology for academic excellence and financial growth.



#### WINS continued:



The Ivy League also saw the following benefits:

**Increased visibility into research data:** Vault provides a centralized view of all research data, which made it easier for the school to track and manage data.

**Improved data governance:** Vault helped the school to implement data governance policies and procedures, which helped to ensure that research data was used and managed in a responsible way.

**Increased research agility:** Vault made it easier for researchers to access the data they needed, which helped to speed up research and make it more efficient.

**Improved researcher satisfaction:** Researchers were satisfied with the security and ease of use of Vault, which helped to improve their productivity and morale.

Overall, the Ivy League university was very satisfied with the results of its journey to integrate Kubernetes with HashiCorp Vault and traditional applications on a private cloud. Under the guidance of the RPT Accelerator, the school was able to achieve its business goals and improve the security, compliance, collaboration, and efficiency of its research environment. They have since renewed their subscription to the RPT Accelerator and with the guidance of RPT continue to maximize the value derived from their tech investments.

## **FUN FACTS**

- 68% of organizations feel vulnerable to insider threats, with 59% experiencing at least one insider attack in the past 12 months.
  -Insider Threats 2020
- The average cost of a data breach was \$3.86 million globally. The study also revealed that it took an average of 280 days to identify and contain a data breach.

## **ABOUT RIVER POINT TECHNOLOGY**

River Point Technology (RPT) is an award-winning cloud consulting, training, and enablement provider, that partners with the Fortune 500 to accelerate their digital transformation journeys and redefine the art of the possible. Our world-class team of IT, cloud, and DevOps experts helps organizations leverage the cloud for transformative growth through prescriptive methodologies, bestin-class services, and our trademarked Value Creation Technology process. From consulting and training to comprehensive year-long RPT Accelerator programs, River Point Technology empowers enterprises to achieve Day 2 success in the cloud and maximize their technology investments.