



Compounding returns through automation

Riverty, a leading financial services provider, uses the HashiCorp suite to deliver a single, automated provisioning workflow and protect sensitive data

About Rivery

Rivery brings a new era of financial freedom to individuals and businesses by innovating with the financial needs and concerns of its customers top of mind. With more than 4,000 employees across Europe and North America, the fintech company combines technology, data, and process optimization to deliver the next generation of financial solutions to thousands of merchants and over 28 million consumers worldwide.

28M+ global customers

80M+ monthly transactions

50-75% faster ticket resolution with self-service IaC

Accelerated pull request approvals from days to hours, reducing approval time by 80%

10x faster infrastructure deployment: days → hours

Real-time security management: Zero expiration incidents

Modernizing legacy fintech infrastructure

Powering over 80 million transactions each month, Rivery delivers flexible payments, debt collection, and smart accounting solutions while constantly pushing to innovate. But sustaining that scale demands sharp operational efficiency, especially within IT. To meet rising demands, the company had to modernize its legacy IT infrastructure and reengineer development practices within a hybrid cloud environment to boost agility, security, and compliance.

Operational overhead causes development delays and risk

With millions of users relying on Riverty's digital payment solutions across 5,000 online shops, availability and speed are non-negotiable. To meet those expectations, Riverty's 250 Pay and Credit engineers are responsible for building and maintaining high-availability APIs that ensure seamless, always-on access regardless of when or where users engage.

But for years, the team operated within the limits of an on-premises IT strategy, where infrastructure was managed by a central technology team that served as the full-service provider for development teams across the organization. With dozens of teams working on multiple products, infrastructure requests — from provisioning environments to updating secrets and certificates — piled up fast, slowing time to market. Engineers often waited days for support tickets to be resolved, delaying delivery and creating unnecessary friction in the build process.

“Our small team can't be the bottleneck for our large, growing organization where demands on us are increasing,” says Stephan Kürpick, Technical Unit Lead, Pay and Credit at Riverty.

Secrets management was another growing pain. The central infrastructure team handled secrets manually in Azure Key Vault, often leading to a backlog. Combined with Riverty's decentralized structure, this manual approach increased the risk of secret sprawl, expired credentials, and overlooked updates, posing serious compliance and auditing risks.

To move faster without compromising on security, Riverty needed to rethink its development workflow. “We needed a solid, reliable, self-service infrastructure and unified workflow for all of our development teams,” says Pavel Ozerov, Technical Program Manager at Riverty.

Challenges



Development bottlenecks caused by a ticket-based infrastructure provisioning model



Operational inefficiencies from inconsistent, manually managed environments



Slow time to market due to long provisioning cycles and limited developer autonomy



Increased risk of downtime and non-compliance from static, inconsistent infrastructure configurations



Security exposure from manually managed secrets and expired credentials



Limited agility and high cost from vendor lock-in and lack of provisioning portability



Compliance risks from poor visibility and fragmented management of secrets and certificates

“We felt that HashiCorp had a solid finger on the pulse of what our engineers need and like to work with. Our engineers simply like interacting with their platforms.”

Stephan Kürpick

Technical Unit Lead, Pay and Credit,
Riverty

Investing in speed and scalability

Riverty needed a platform that could streamline infrastructure and security management while meeting developer expectations — all without the overhead of building everything from scratch. They found that in HashiCorp. “We felt that HashiCorp had a solid finger on the pulse of what our engineers need and like to work with,” says Kürpick. “Our engineers simply like interacting with their platforms.”

Implementation speed was also a key factor in Riverty’s decision. “We wanted to quickly implement this infrastructure platform for our engineers rather than taking significant time building and customizing it ourselves,” says Ozerov. “HashiCorp provided us much of what we needed right out of the box, allowing us to optimize our engineering time during implementation.”

With HashiCorp as its foundation, Riverty fast-tracked both its cloud migration and transition to a DevOps operating model, enabling engineers to work more independently while reducing operational risk and inefficiency. Since the company relied on a global, multi-cloud environment spanning Microsoft Azure and Kubernetes, maintaining infrastructure consistency was critical.

To address this, Riverty adopted HCP Terraform to standardize infrastructure as code and automate provisioning workflows. Instead of relying on manual processes, development teams now use reusable, self-service templates that allow them to spin up infrastructure on demand, accelerating delivery without sacrificing control.

“Developers don’t have to wait for a central team to provision the infrastructure for them, which previously took hours or sometimes days,” says Ozerov. “Now, teams use pre-configured modules and the magic happens. This greatly simplifies life from an infrastructure standpoint, and it’s made a huge difference.”

HCP Terraform also bridges provisioning skills gaps for Riverty. With reusable HCP Terraform modules, engineers can quickly deploy pre-approved standard infrastructure components or build custom templates aligned with internal policies, all reviewed through a streamlined pull request (PR) process to ensure consistency and control. This standardization supports Riverty’s business operations by reducing risk and potential downtime that can result from configuration errors, while also meeting compliance demands such as backup and recovery requirements.

“When we develop a module for an infrastructure component such as an SQL Server and database, we define the default policy for the backup,” says Ozerov. “Then, when various parameters and values are applied to that module by engineers, the backup policy isn’t forgotten. It’s inherent, which is extremely important for compliance.”

“With Vault, we’ve addressed our big risk of secrets expiring head-on,” says Ozerov. “The more we can automate, the more secure and compliant we become, plus it makes our lives easier as engineers. In fact, since implementing Vault, I haven’t received a single notification that a secret has expired.”

Pavel Ozerov

Technical Program Manager, Riverty

Hedging against credential risk

Expanding on its efforts to remain compliant, Riverty also adopted HashiCorp Vault to protect sensitive data and manage secrets at scale. Vault now serves as the system of record for the full lifecycle of secrets, certificates, passwords, and encryption keys. The team redesigned its security management approach to align with strict auditing and regulatory requirements such as PCI DSS, implementing role-based access controls to isolate infrastructure components and enforce least-privilege access.

Today, Riverty centrally manages over 430 secrets through Vault, including 150 dynamic secrets (primarily database and RabbitMQ credentials) and 285 static secrets. Dynamic secrets are generated on demand and expire automatically, while static secrets are stored and rotated through Vault's secrets operator using a trigger. All of this has contributed to a significantly faster and more secure credential management process. Vault also handles certificate generation and revocation on demand, further reducing manual overhead and improving security posture.

"With Vault, we've addressed our big risk of secrets expiring head-on," says Ozerov. "The more we can automate, the more secure and compliant we become, plus it makes our lives easier as engineers. In fact, since implementing Vault, I haven't received a single notification that a secret has expired."

Keeping the modernization momentum going

To stay ahead, Riverty also plans to implement HashiCorp Consul to standardize service networking and automate connectivity across dynamic, multi-cloud environments. With services increasingly distributed across Kubernetes clusters and cloud providers, the business needs a more flexible way to map service relationships and define clear, enforceable communication policies between internal and external systems. Consul service discovery and service mesh capabilities will play a key role in supporting that evolution.

Another big initiative underway for the team, besides modernizing the infrastructure, is infrastructure harmonization. “We’re currently working on the future setup of our infrastructure by migrating all components still located in on-premises datacenters to the cloud. We will then optimize the whole environment, not only from a technical but also from a business point of view, to deliver wider benefits to the organization, like reducing costs.”

Financial technology for a new era

With a continually improving infrastructure at its core, Riverty is now better equipped to not just deliver flexible financial solutions to customers but to drive innovation for a new era of financial technology. The HashiCorp Cloud Platform supports Riverty's most critical applications while enabling engineers to go to market faster and more securely.

"The infrastructure as code offered by HCP Terraform is key to keeping everything secure, compliant, and structured," says Ozerov. "Everyone knows the boundaries of responsibility; they know how things are configured, how to make a change, and how fast that change will be delivered. That's a game changer."

Outcomes



Cut support ticket resolution time from one day to a few hours with self-service IaC



Reduced infrastructure change rollout from a few days to same-day via pull-request-based workflows — a 90% reduction in deployment time



Accelerated pull request approvals from days to hours, reducing approval time by 80%



Enabled multiple infrastructure updates per day, saving hundreds of engineering hours quarterly



Eliminated service redeloys for secret rotation across 150+ credentials



Automated secrets management, removing the risk of expired credentials



Freed up the development team to focus on strategic projects by automating infrastructure provisioning and security management



Standardized deployments across Azure, AWS, and Kubernetes, avoiding vendor lock-in

Riverty turned to HashiCorp to modernize its IT infrastructure, provide greater efficiency through automation, elevate its security and compliance, and go to market faster.

Solution

Riverty Partners



Stephan Kürpick
Pay and Credit
Technical Unit Lead



Pavel Ozerov
Technical Program Manager

© Copyright IBM Corporation 2025

August 2025

IBM, the IBM logo, HashiCorp, Vault, and Terraform are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

