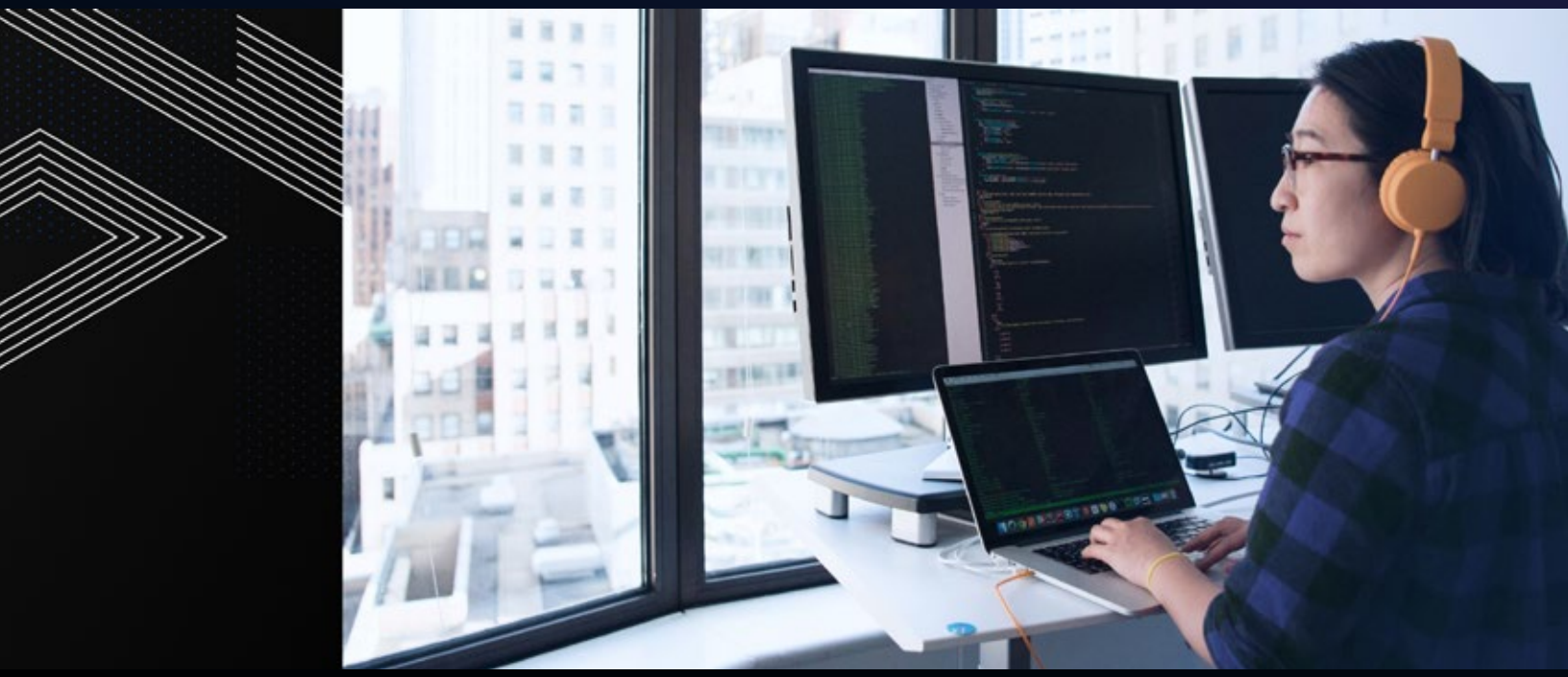
HashiCorp



CASE STUDY

Running HashiCorp with HashiCorp

HashiCorp's engineering services uses the HashiCorp software stack to gain control and agility in application deployments.

// Infrastructure Enables Innovation

HashiCorp Summary

HashiCorp provides infrastructure automation software for multi-cloud environments, enabling enterprises to unlock a common cloud operating model to provision, secure, connect, and run any application on any infrastructure. These solutions allow organizations to deliver applications faster by helping enterprises transition from manual processes and ITIL practices to self-service automation and a DevOps approach. All of HashiCorp's foundational technologies are open source and developed collaboratively, and have been since the company's founding in 2012.

FAST FACTS

1,700 Customers

10M requests per day on Nomad cluster

60%+ reduction on third-party PaaS costs

Reduced operational complexity

100% success rate for ~30k Vault requests per day

Deploy, build, and migrate with zero downtime

> Now, we can ship a change, have it automatically stage, then deploy and redeploy every instance in the entire stack with all of our applications migrating seamlessly across nodes, without any downtime."

JEFFERY HOGAN
SENIOR INFRASTRUCTURE ENGINEER
HASHICORP

Applying our tools to our systems

Over the years HashiCorp has grown into a global leader helping companies provision and manage infrastructure using its open source infrastructure as code offerings. Today, more than 150 of the Fortune 500 and more than 1,700 organizations from around the world rely on HashiCorp's multi-cloud infrastructure automation products.

Building and managing our products requires complex coordination behind the scenes. HashiCorp's own Engineering Services Group plays a key role in managing the various systems and platforms for internal and external users. While HashiCorp internal teams had made pragmatic choices in the past to use various software solutions where appropriate, our Engineering Services Group had a growing recognition of where HashiCorp Consul, Nomad, and Vault could improve upon the status quo.

"We really wanted to manage our systems without a need for compromises and without expanding the scope and type of platforms we were obligated to support," says Jeffrey Hogan, senior infrastructure engineer at HashiCorp. "We wanted to create a universal way of tackling these sorts of challenges with our own packaged HashiCorp solutions and systems that previously we'd been using multiple other vendors or platforms to address.

Limited visibility meant limited control

Behind the curtain of HashiCorp's rapid expansion, the Engineering Services Group maintains the internal systems to support other teams within the organization. The small team is tasked with building and deploying internal apps for continuous integration, maintaining the functions of HashiCorp's public cloud platform, and supporting users across the organization to ensure services are available, performing as they should, and in compliance with data and security standards.

Over the years, the team used HashiCorp's own products in a number of ways but continued to rely on an array of third-party platforms to orchestrate and manage internal systems. For example, the team had used a third-party orchestrator to manage, deploy, and scale applications as well as balance workloads.

"As a small team with limited bandwidth, we chose to optimize for speed early on when scale and complexity were relatively modest, using established tools while we worked on enhancing our own," Hogan says. "But over time, the volumes became greater, which also carried over to our networking efforts, and the pain of the status quo became acute and made us take another look.

Not only was the volume of work increasing, but the complexity was as well. The use of disparate tools meant there was no way to fine-tune their secrets management policies and procedures, like defining when secrets are rotated or when they expire, the team had to manually manage dozens of secrets that consumed significant time they could've spent on more critical activities.

"We recognized a lot of these challenges were the same ones that our customers use our products to solve every day, which made for a compelling and very straightforward case for us to reconsider our own approach," Hogan explains. "Both our products and our company have grown and matured since those days and it became obvious that we could (and should) have our products take a much more comprehensive role in our business."

Challenges

Standardizing infrastructure and secrets management onto a single platform as the business grew

Adapting workflows for greater efficiency and team productivity

Enhancing secrets management operations and improving response times to incidents

> Using the HashiCorp stack gives us a consistent deployment platform that allows for a more dedicated focus on improving developer and operator experiences."

JP TOTO
ENGINEERING MANAGER
HASHICORP

Reducing time, effort, and mental overhead

Many of our workflows and processes have been around as long as the company — and in some cases, longer than even some of our own products. Out of necessity and expedience for serving evolving customer needs, we opted for established third-party tools to support everyday operations. But as our company grew rapidly and the volume and complexity of our customers' needs evolved, the team recognized the benefits of making clean break from third-party tools and consolidating to the HashiCorp solutions that large organizations around the world rely on instead.

With the HashiCorp stack — Terraform, Consul, Nomad, and Vault specifically — the team has a comprehensive end-to-end toolset that enables them to stand up infrastructure, launch and connect microservices, and manage secrets across both on-premises and AWS cloud environments. Each part natively interoperates with the other parts, making it a much smoother, integrated, efficient workflow.

"Replacing our third-party tools with the HashiCorp stack helped us standardize the entire environment to give us better control and agility across the board," says JP Toto, engineering manager at HashiCorp. "After a methodical initial deployment and configuration, we now have the ability to automate a range of previously manual secrets-related operations while also monitoring our various server clusters in real-time to quickly respond to and resolve potential issues without interfering with our users' experiences."
"The open source-to-enterprise transition with Vault was critical for us, as it gave us the chance to re-engineer our secrets management practices with little or no financial investment and then strategically begin paying for the tools and capabilities we actually needed instead of buying into a one-size-fits-all solution like many Vault competitors offer," he says. "More importantly, it gave us a centralized and secure secrets management platform capable of supporting multiple cloud regions throughout Asia on Google Cloud Platform for better resilience, easier scale, and effortless secrets management."

Slow and steady wins the race

The team took a deliberate and modular approach to their transition away from third-party tools, letting them learn best practices as they went along. They started migrating extant systems with fewer business-critical applications to run using the HashiCorp stack bit by bit, allowing them to gain operational experience in production.

The transition started modestly, deploying Vault to handle authentication for the internal stack instances. Then they expanded to enable easy scale-out and scale-in instances without the time-consuming manual credential bootstrapping required by the former secrets management solution.

"Vault gives us the flexibility and fine-grained secrets management control to grant temporary credentials for somebody to audit a database or system, automate secrets updates, or manage batches of secrets however we want or need," Toto says. "For example, if secrets are inadvertently leaked somehow, we know they're just going to expire anyway and we can invalidate all of them in a batch, which brings us much closer to the zero trust environment we've been aiming to create for years."

After a successful run with Vault, the team determined it had also worked out a decent pattern for managing the underlying infrastructure and configuration using Terraform and Packer. They leveraged that knowledge to relatively quickly stand up Consul and Nomad clusters alongside Vault.

"We started with simple recurring background tasks in Nomad, doing things like retrieving application credentials from Vault and then expanded that into low-priority and internally facing web applications," Hogan explains. "It allowed us to gain experience enabling HTTP ingress for Nomad jobs as well as monitoring and operating it day-to-day that we could apply when we started deploying higher-value, more important web applications later on."

Hogan says that the runtime environment created with Nomad or Consul makes it easier than ever to run experiments or pre-production services at any time because if parts of the clusters break, they'll come back online without interrupting service. It gives the team peace of mind that they can add new services in an environment the security team has validated for them.

"The fact we can have our Nomad or Consul clusters sit for two weeks and not worry about them breaking because they come back online without interrupting services, means we can have Nomad and Consul available to fulfill any sort of runtime networking," he explains. "Now, we can ship a change, have it automatically staged, then deploy and redeploy every instance in the entire stack with all of our applications migrating seamlessly across nodes, without any downtime."

A new standard for today and tomorrow

Adopting the HashiCorp stack has fundamentally reshaped the way our internal teams operate. Moving to using HashiCorp's own products replaced the hodgepodge of third-party solutions, while offering a greater number of features and functionality. At the same time, the move has significantly reduced the amount of time and effort — and cost — of onboarding new teams and their workloads, since they're already familiar with the tools used in customer deployments.

With the HashiCorp stack, the team also has more granular control over every aspect of the IT environment. Toto says that it took just six months for the group to go from having no direct usage of Consul, Nomad, or Vault to the HashiCorp stack being their default choice of deployment platform. More importantly, he says that even with just two engineers involved at any given time, the HashiCorp stack has enabled the team to make material improvements to their workflows that have boosted productivity, efficiency, and overall skill development.

"Using the HashiCorp stack gives us a consistent deployment platform that allows for a more dedicated focus on improving developer and operator experiences," he says. "We've virtually eliminated manual management of entire classes of credentials like AWS access keys. We've replaced other manual infrastructure management with automated scaling in Nomad for horizontal node scaling and dynamic application sizing. With Consul, we automatically connect the microservices we've deployed."

Overall, both Toto and Hogan agree that opting to use the HashiCorp stack has significantly increased the team's work capacity. It also delivers a better engineer experience due to its greater flexibility and a lack of undesirable compromises they were forced to make in the past. "I've been in lots of other situations where a transition like this would have been a pipe dream that wasn't achievable in reality," says Hogan. "As an engineer first, it's been one of the most joyful things to work on."

Outcomes

Automated secrets lifecycle for dozens of secrets and cloud credentials

Deployed changes, new builds, and app migration across nodes with zero downtime

Enabled more experimentation and semi-production services

Enhanced institutional knowledge and overall team skills by adopting the company's own tool stack

Solution

HashiCorp uses our own HashiCorp stack for end-to-end visibility, greater control, and automation across its internal engineering operations.

HashiCorp Partners

JP is the manager of engineering systems at HashiCorp. He has over 20 years of experience as a software engineer where he has worked in pharma, fintech, and various startups. JP is passionate about the DevOps value proposition and automation tooling and even authors and maintains open source training.

Jeffrey is a senior infrastructure engineer at HashiCorp and is a seasoned DevOps professional. He maintains the most widely used Vault API client Python library (HVAC) and prior to HashiCorp, was an infrastructure engineer supporting a large PaaS (WP Engine) and their fleet of 10,000 virtual machines.

Technology Stack

- **Infrastructure: AWS EC2 Autoscaling Groups**
- **Workload type: Periodic background tasks and web applications**
- **Container Runtime: Docker**
- **Orchestrator: HashiCorp Nomad**
- **CI/CD: CircleCI and GitHub Actions**
- **Data Service: Various AWS stateful services (RDS, DocumentDB, etc.)**
- **Service Mesh: HashiCorp Consul**
- **Version Control: git**
- **Networking: AWS EC2**
- **Provisioning: HashiCorp Terraform**
- **Security management: HashiCorp Vault**


HashiCorp