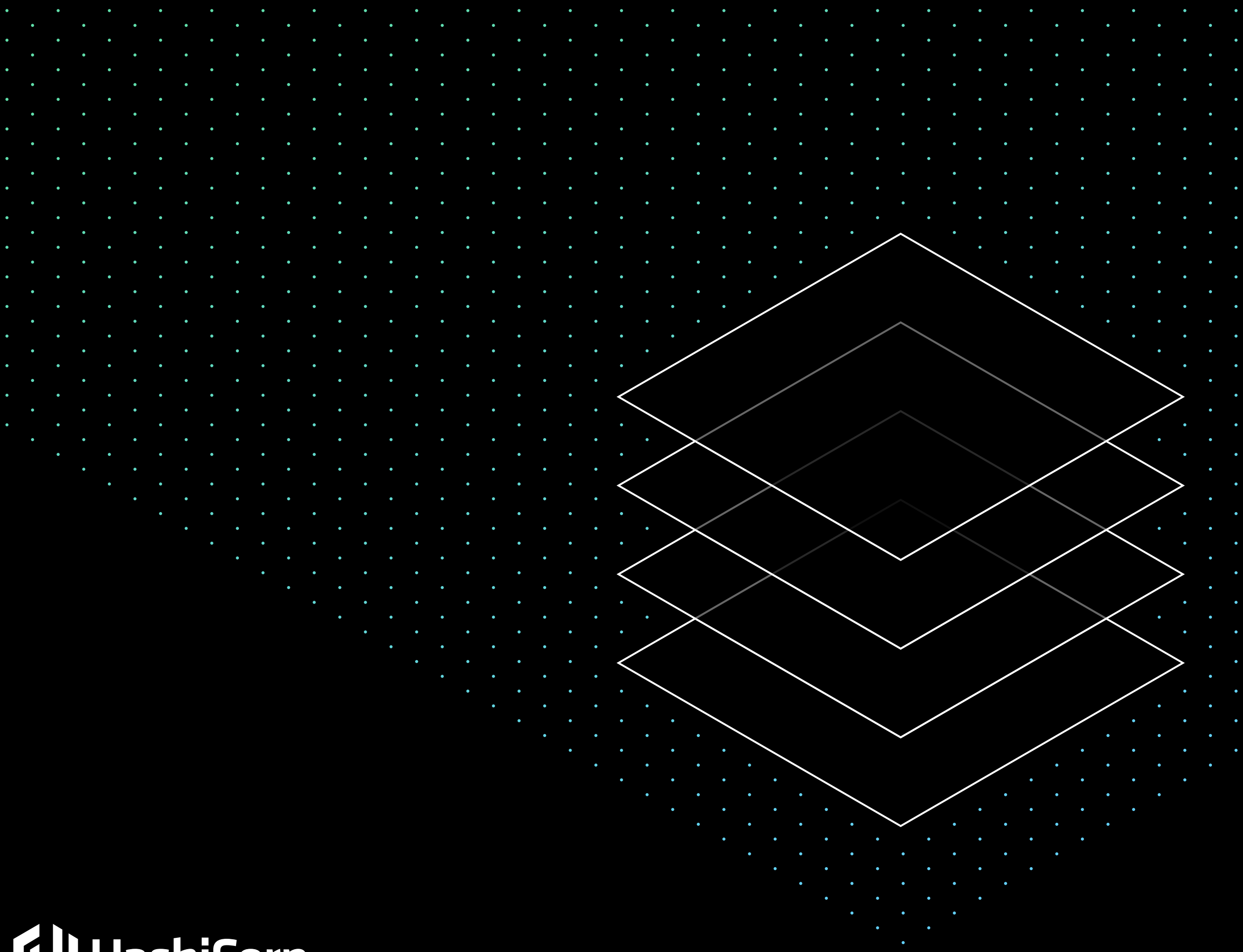


HashiCorp

Deriving Business Value from the Cloud Operating Model in the Public Sector

Assessing the risk of current operating models in a cloud-first strategy

Whitepaper

Contents

Executive summary

Organizations in both the public and private sectors are increasingly embracing cloud as a way to accelerate their digital transformation. In a recent survey of cloud trends, over 93% of the respondents stated that they have a hybrid, cloud-first strategy. In that survey, the respondents technology leaders stated that a cloud strategy is necessary for the long term viability of their respective operating models.

In a different survey by Logic Monitor, 87 of respondents stated that the global pandemic will accelerate time tables for cloud adoption. These leaders understand that the risk of continuing the current way of delivering technical value is not going to meet their needs over the next decade.

In this need to move to the cloud and in implementing the new operating model that this change requires, these leaders have run into significant headwinds. There are three main areas of risk:

1. **Costs & Control:** How do organizations manage cloud spend and budgets when infrastructure is on-demand, every developer is a buyer, and services are virtually unlimited, deployed frequently, and onto many target environments?
2. **Skills & Productivity:** How do organizations leverage the finite skill pool and keep employees productive across the growing scale and complexity of the enterprise?
3. **Boundaries & Risk Mitigation:** How do organizations secure and connect their assets across permeable boundaries?

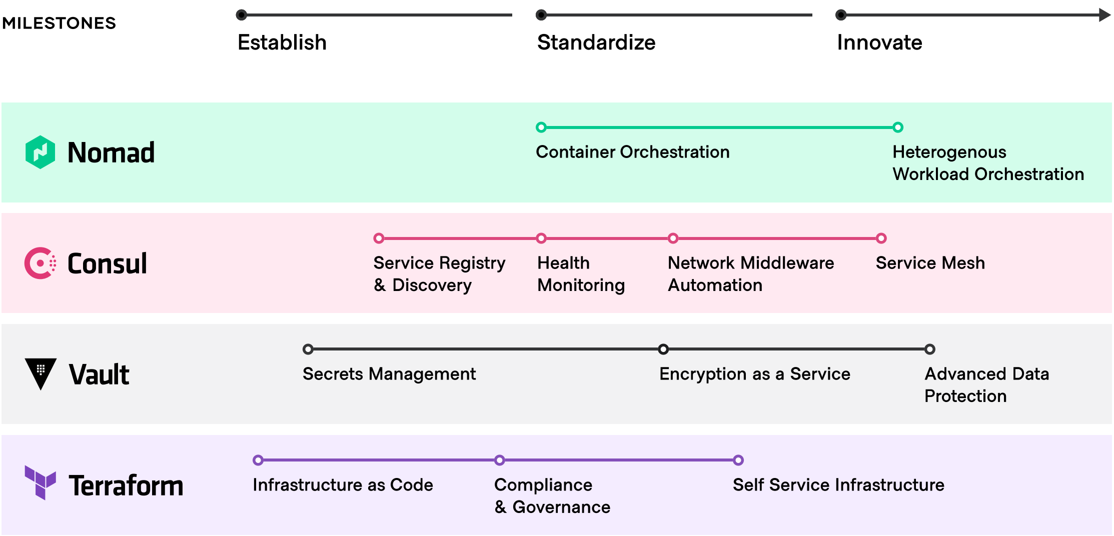
The implication of these answers can determine the success or failure of cloud adoption and digital transformations. This was revealed in a recent Forbes article that said 7 out of 10 digital transformations were deemed a failure by senior leaders.

In this white paper, we will address these questions, the risk associated with them and what can be done to avert a poor outcome for organizations leveraging HashiCorp products to implement a cloud operating model for digital transformation.

Digital transformation is a journey not a project

Most IT organizations work from project to project. These projects flow out of initiatives set at the leadership level and then translated into discrete projects with deadlines and prioritized based on need. This is not the case with a digital transformation where it is an adjustment to the operating model that impacts people, processes, and tools. For organizations, there is a consistent pattern to the journey that helps achieve digital transformation through the adoption of cloud: build cloud essentials, standardize through shared services, and innovate by applying the common architecture to new clouds, use cases, lines of business. This journey can be applied to each layer of infrastructure and application delivery: core infrastructure, security, networking, and application service delivery.

Example of enterprise journey to unlock a Cloud Operating Model



Each one of these journeys is an initiative in its own right. As discussed in the Cloud Operating Model white paper, this means delivering new institutional and customer value more quickly, and at a very large scale. The implication for IT then is a shift from cost optimization to speed optimization.

As with adoption of any new technology, cloud also brings additional or new expenses related to software, training, implementation, support and maintenance. However, there are significant cost benefits associated with cloud adoption that are often not directly implied and hence not attributed as a benefit.

There are many examples of organizations that have successfully moved away from traditional methods to digital engagement with their users:

- **Roblox:** By leveraging **HashiCorp Nomad**, they were able to reduce new application deployment from 8 weeks to 8 minutes, while reducing onboarding time for new developers to 30 minutes. This also resulted in a savings of over **$10 million** in Windows licensing fees due to reduced need for running non-containerized Windows apps and optimizing resources.

- **TMX:** Leveraged **HashiCorp Terraform** accelerate and automate infrastructure provisioning across multiple business areas while also standardizing their deployment methodologies. Resulted in reusable templates and processes that decreased time to deployment and manual processes saving money and allowing developers to focus on business critical tasks.

- **Athena Health:** Through the integration of **HashiCorp Vault**, consolidated the management secrets and records over **40% of U.S. patients**. This resulted in significant cost savings through the securing and automation of secrets management with more that **3 million** requests per day.

- **Criteo:** Employed **HashiCorp Consul** to automate discovery and connectivity among various microservices on their private DCS, helping the organization enhance its service monitoring and overall performance across the enterprise as well. This reduced infastruce cost by millions of dollars and reduced server spin-up time from hours to seconds.

The journey for many, especially the early adopters, was not easy but they have paved the way for many more to follow. From retailers to government agencies, there are many areas that have benefited from digital transformation.

But what exactly constitutes success? The best indicators in the public sector are:

- Increased speed of development
- ROI for software investment, development and deployment
- Overall decrease in cost over time
- Greater security
- Reliability and standardization of systems for internal and contractor resources
- Easier collaboration across organizations
- Automation of manual tasks

These allow DevOps and development teams to focus on value driving task resulting in a stronger user experience that is directly aligned to overall digital transformation efforts.

The United States Federal Aviation Administration (FAA) experienced many of the struggles that can arise from while attempting their own digital transformation. As they began the process of transitioning application and development to the cloud, they initially encountered cumbersome, manual workflows that were difficult to integrate with their existing infrastructure or additional clouds. This resulted in slow, inconsistent infrastructure built upon a great deal of code that was risky to change or update.

By leveraging Terraform Enterprise and employing infrastructure as code they were able to quickly move beyond these challenges and begin seeing the true value of moving to a cloud based infrastructure. Infrastructure provisioning became simple and easily reproducible, resulting in both greater agility of app development and developer onboarding. In addition, Sentinel policies ensure policy compliance, consistency, and security across all developer environments. As a result of leveraging HashiCorp products they were able to both migrate more than 200 apps to the cloud while also establishing the infrastructure they would need to build future applications there as well.

Examples like this display how by adopting cloud computing and being fully invested in leveraging the right tools to support this digital transformation, organizations can vastly improve their DevOps processes allowing for quicker development, deployment and updating of mission critical applications.

Preparing for digital transformation with automation

As organizations decide to make the transition to the cloud, it is important to understand and prepare for some of the changes. The fundamental change is the shift from "static" infrastructure to "dynamic" infrastructure: from a focus on configuration, and management of a static fleet of IT resources, to provisioning, securing, connecting, and running dynamic resources on demand.

Decomposing this implication, and working up the stack, various changes of approach are implied:

- **Provision.** The infrastructure layer transitions from running dedicated servers at limited scale to a dynamic environment where organizations can easily adjust to increased demand by spinning up thousands of servers and scaling them down when not in use.

- **Secure.** The security layer transitions from a fundamentally "high-trust" world enforced by a strong perimeter and firewall to a "low-trust" or "zero-trust" environment with no clear or static perimeter.

	Static		Dynamic
Run	Dedicated Infrastructure	→	Scheduled across the fleet
Connect	Host-based, Static IP	→	Service-based, Dynamic IP
Secure	High trust, IP-based	→	Low trust, Identity-based
Provision	Dedicated servers, Homogeneous	→	Capacity on-demand, Hetergeneous

- **Connect.** The networking layer transitions from being heavily dependent on the physical location and static IP address of services and applications to using a dynamic registry of services for discovery, segmentation, and composition.

- **Run.** The runtime layer shifts from deploying artifacts to a static application server to deploying applications with a scheduler atop a pool of infrastructure which is provisioned on-demand.

Additionally, each cloud provider has its own solution to these challenges. For IT teams, these shifts in approach are compounded by the realities of running on hybrid- and multi-cloud infrastructures and the varying tools each technology provides.

According to a Gartner automation survey of organizations transitioning to the cloud, 63% see workloads increasing but only 44% see development teams increasing and 33% see operations teams increasing.

So for cloud computing to work, automation efficiency is of the utmost importance.

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. The HashiCorp suite enables organizations to adopt the products in a way that aligns to the digital transformation journey (build, standardize, innovate).

Why HashiCorp?

HashiCorp pioneered the creation and use of cloud infrastructure automation, providing consistent workflows to provision, secure, connect, and run any infrastructure for any application. Adobe, Barclays, Pandora, Hulu, Roblox, and Cloudflare are some of the more than 1,500 enterprises we have helped to transition from manual processes and ITIL practices to self-service automation and DevOps practices.

HashiCorp's tools provide a control plane for each layer of the cloud, enabling organizations to make the shift to a cloud operating model. Each product addresses specific technical and organizational challenges of cloud infrastructure automation.

- **Provision with HashiCorp Terraform**: Use reproducible infrastructure as code to provision any cloud, or infrastructure.
- **Secure with HashiCorp Vault**: Manage secrets and protect sensitive data.
- **Connect with HashiCorp Consul:** Automate service-based networking in the cloud.
- **Run with HashiCorp Nomad:** Deploy and manage any containerized, legacy or batch application.

Expanding use of the HashiCorp Stack increases maturity and velocity for our customers

Provision / Operations	**Secure** / Security	**Connect** / Networking	**Run** / Deployment
Terraform	**Vault**	**Consul**	**Nomad**
Hybrid Cloud **Infrastructure Automation**	Hybrid Cloud **Security Automation**	Hybrid Cloud **Networking Automation**	Hybrid Cloud **Application Automation**
Infrastructure as code	Identity-based security	Common service registry	Workload orchestration
Compliance & management	Secrets management	Service discovery	Container orchestration
Self service infrastructure	Encryption as a service	Network middleware automation	Hetergeneous orchestration
	Advanced data protection	Zero trust networking with service mesh	

In many ways, HashiCorp tools are both the pathway to cloud adoption and once there, it's the backbone to ongoing operations in the cloud.

Organizational business outcomes using HashiCorp Cloud Infrastructure Automation

In the context of digital transformation, there are primarily two major initiatives that organizations undertake, both of which involve HashiCorp's cloud infrastructure automation products -

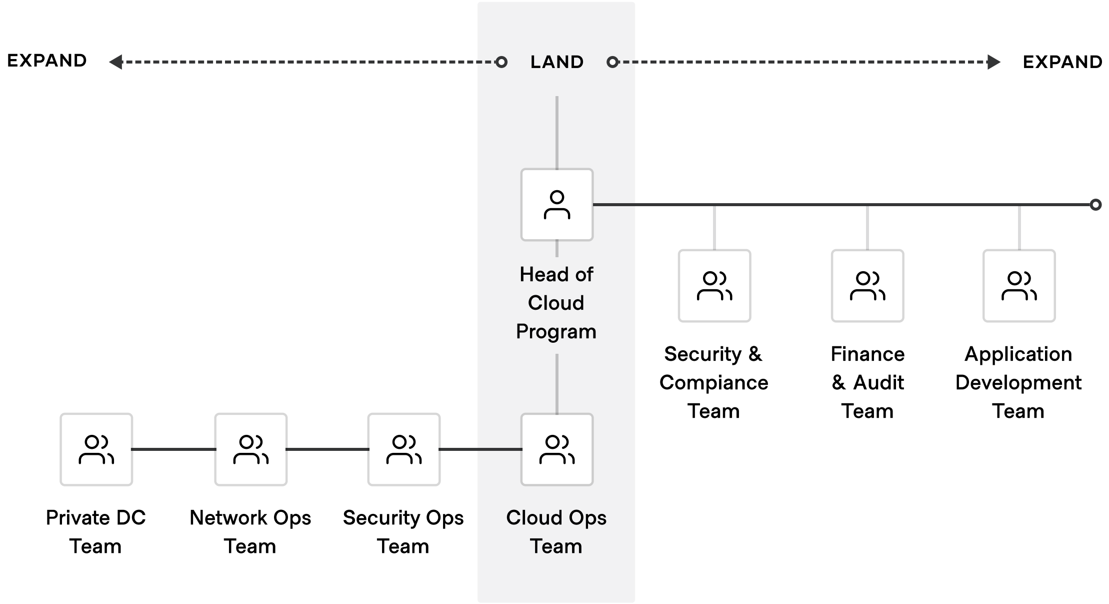
1. Infrastructure modernization (cloud migration)
2. Application workload delivery

While these initiatives require initial investments, the business outcomes over short and long term more than pay for itself. The buckets of value are:

1. Productivity improvements
2. Cost optimization
3. Risk mitigation

Productivity improvements

Adopting infrastructure automation helps organizations increase productivity: Terraform provisions infrastructure in minutes instead of weeks.   Vault automates, controls, and secures infrastructure through centralized management tools. With Consul, organizations can accelerate the development of new applications by discovering and connecting services from weeks to minutes.   Nomad allows for the quick and easy deployment of software in minutes with minimal developer onboarding. The challenge that most organizations run into quickly is once the essential workflow is established, how does the rest of the organization adopt it?



With the organization there are many teams who are participants and stakeholders in the digital transformation journey: operations, security, application development, compliance and audit, and finance. For many, the organizations looks like this:

This results in siloes of people, process, and tools when the organizations embark on the digital transformation. The Cloud Team often builds out essential workflows that do not align with the needs of stakeholders teams, which results in multiple teams building out their own core workflows. If you look at each layer of the operating model (infrastructure, security, networking, runtime) this creates inefficiencies in productivity due to:

- Many workflows being learned, managed, governed, and audited
- Manual hand-offs between operations, security, development, and finance
- Lack of sharing and reuse, meaning many individuals are doing the same work

Not solving these challenges around productivity negatively impacts the efficacy of teams to ship new innovations to users and customers. For example, State of DevOps report, 79% of respondents needed days or weeks lead time, even up to 6 months for lower performing organizations, to prepare for deployment tasks. This is orders of magnitude slower than the schedule that development teams plan for shipping new enhancements to the customer experience in their applications.

These challenges are further compounded by the adoption of multi-cloud, adding more complexity to the equation. According to a Gartner survey, enterprises use an average of 5 clouds, with three being used in production and two for development and test.

With the HashiCorp suite, infrastructure automation addresses the concern of manual tasks and the individual products address the concern of workflow consistency across teams, providing the ability to easily share, collaborate on and reuse projects, and work across public cloud, private datacenters, and a variety of other infrastructure and applications types.

In general, organizations can expect to increase productivity by up to 80% due to consistent, automated workflows across all teams, and codified workflows that make debugging and issue resolution minimal.

Organizations are able to reassign full-time employees to new projects aligned to creating value for the organization rather than repetitive manual tasks that represent lost dollars to support a legacy status quo. This equates to millions of dollars annually along with increased productivity and the ability to focus on core organizational goals.

Evidence:

Infrastructure Provisioning

A major insurance carrier was able to identify 500 hours of manual tasks each week that could be eliminated across 15 FTEs due to manual provisioning, security and compliance policy checks, and issue resolution. The estimated spend saved associated with each FTE that was ~$2,000 / weekly and company spend was ~$30,000 / weekly (or $1.5M annually).

Infrastructure Security

Athena Health is a global leader in healthcare technology and by using Vault was able to enhance security and keep its partner and customer records in tip-top shape by consolidating multiple homegrown systems into a single service servicing 300 million secrets a day for 40% of US healthcare customers.

Infrastructure Networking

Criteo is a leading global advertising platform and aggregates data from 75% of the world's online shoppers. Criteo uses Consul to launch new services in <1 minute (a process that previously took 3 weeks) by eliminating all manual operations.

Cost optimization

A long-term challenge for cloud adoption is managing cloud spend within a budget that fits the operating costs that is acceptable to the organization's operating model.

During the initial phase of the journey, the central cloud team owns and manages most of the workflows that touch cloud; however, the ultimate goal is that application developers are in the driver's seat, provisioning and managing their own infrastructure. This idea of self-service workflows for developers is the underpinning of the initial innovation phase that is often part of the cloud adoption process. However, without proper guardrails to ensure teams operate with a cost-efficient mindset, organizations will find themselves spending up to 40% on unused and over-provisioned resources and Gartner expects that organizations will spend more than $15 billion on provisioned but unused cloud infrastructure. These are the things that are making the long-term viability of cloud challenging. According to the 2021 State of Cloud report, organizations report the following trends:

- 90% of organizations report they were over-budget for their cloud spending due to the Covid-19 Pandemic

- 79% of respondents listed managing cloud spend as one of their key challenges.
- More than 50% of respondents are still using either cumbersome manual processes, or have do not implement actions and changes to optimize at least some portion of how they manage their cloud resources
- Respondents estimated that over 30% of cloud spend is wasted, displaying the difficulty they have in both managing cloud spend and maintaining visibility into it.

With HashiCorp, the approach focuses on consistent workflows. This allows organizations to consolidate solutions and eliminate operating costs from procuring and managing multiple redundant systems. The approach to automation through codifications makes it easy to build guardrails for cost-mind infrastructure into the process. For example, Terraform modules represent code that is created, tested, and validated by an organization's Cloud team and then can be made available to developers. Each time a developer uses a module to provision infrastructure, it will follow the codified guardrails: embedding time-to-live variables or restricting dev-test to standard compute infrastructure rather than costlier premium set-ups.

In general, organizations can expect to see a 30-40% reduction in cloud spend using Terraform and Consul to understand the state of infrastructure and services at all times, make decisions about what can be deprovisioned or consolidated, or simply just enforce operational best practices within the workflow.

In total, this can be a significant amount of the budget that is wasted into costs that return little to no value back to the business or the digital transformation and that can be easily saved and repurposed. The wasted cloud spend referenced above equals millions of dollars lost due in part to outdated methods of infrastructure management, and unstructured processes that don't properly align to the dynamic nature of cloud.

Evidence:

Core Infrastructure

Organizations see up to a 40% reduction in cloud infrastructure spend using Terraform modules and policies to enforce best practices. Policies that help to reduce unnecessary cloud spend include restricted provisioning of non-production infrastructure during nights and weekends, restricting development and test compute to lower-cost options, use of the time-to-live (TTL) variable, and regular clean-up using centralized infrastructure state records.

Networking Infrastructure

Organizations can see over a 75% decrease in costs of networking infrastructure when using Consul. For example, Criteo has used Consul to reduce a wide range of infrastructure components radically reducing its infrastructure footprint while saving millions of dollars per year in infrastructure maintenance, licensing, and upgrade costs.

Security Infrastructure

Vault helps greatly reduce operational costs relating to secrets management. athenahealth was able to eliminate their old manual ticketing system and establish overarching secrets policies. This allowed the organization to find the proper balance between ensuring the continued security and protection of their sensitive data while minimizing the amount of time and effort it takes to do so.

Runtime Infrastructure

Roblox successfully implemented its containerization strategy, which helps the company to scale efficiently in dollars and personnel. By containerizing their legacy game engine, upgrading to 64-bit Linux CPU, and adopting Nomad as the single orchestration platform, Roblox achieved between 150-200% resource utilization - they ran double the workload on the same hardware, saved over $10 million in Windows licensing, and had zero downtime when migrating application deployments from on-premises infrastructure to AWS.

Risk mitigation

The migration to cloud means teams and organizations are rethinking how to secure their applications and infrastructure. Risk mitigation centers around reducing impact and severity of the occurrence of a data breach and loss. In the past year, there have a been a staggering 3,950 data breaches globally[1] spanning every major industry. Breaches and data loss are now the No. 1 business worry for U.S. CEOs, ahead of competition and recession[2].

The average data breach took 191 days to detect and costs $3.86 million[3]. Companies that have experienced larger breaches are also 28% more likely to experience recurring material breaches over the next two years.

[1] Verizon 2020 Data Breach Investigations Report
[2] Fortune Magazine - U.S. CEOs Are More Worried About Cybersecurity Than a Possible Recession
[3] Ponemon Institute/IBM 2018 Cost of Data Breach Study

Existing ways to secure applications and infrastructure are no longer effective in preventing lateral movement which happens inside “high trust” zones. According to a 2020 Cost of Data Breach study, lateral movement attempts occurred in over 90% of cyber attacks and cloud misconfigurations were a common root cause of a data breach.

At HashiCorp, our security model is predicated on the principle of identity-based access and security. In order for any machine or user to do anything, they must authenticate who or what they are, and their identity and policies define what they're allowed to do. This means that organizations can automate identity-driven controls across machines, users, and networks with HashiCorp products to reduce risk around breaches occurring. HashiCorp's offerings also provide a holistic strategy to secure your applications and infrastructure while providing the means of quickly mitigating.

Evidence:

Infrastructure Security

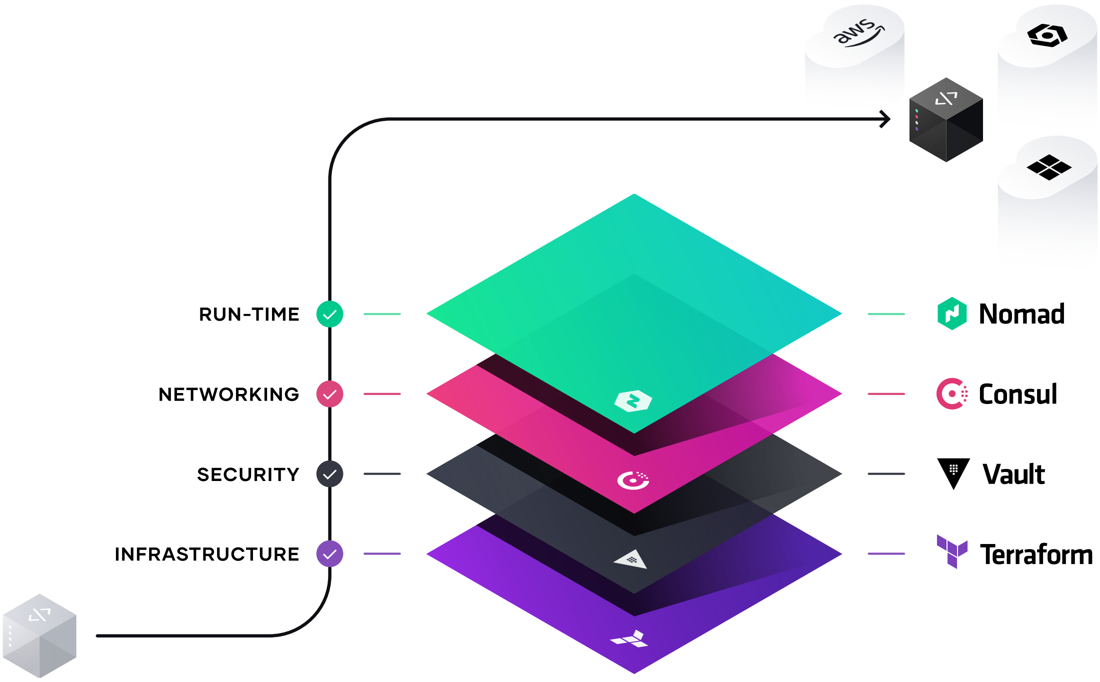
Vaults helps organizations reduce the risk of compromised secrets by aiding them to centralize and then build access control around them. Then, through dynamic secrets management and encryption as a service, it is able to make sure that if credentials are compromised they are short lived and should data be compromised, it will be of no value. For example, at Adobe, they were able to implement Vault to help manage the security and compliance layer of their applications, mitigating sprawl and allowing those developers to focus on their customers as opposed to security risks.

Infrastructure Networking

Consul reduces risk by providing consistent end-to-end security across services while proactively preventing outages and mitigating downtime for business critical applications. It also enables application resiliency through policy-driven traffic routing and load balancing. At Pandora, Consul was able to create a powerful way for developers to operate “least-privilege” access by default.

Summary and conclusion

As organizations aim to deliver digital transformation initiatives across their businesses and make the transition to the cloud, there is a consistent pattern and journey when dealing with the shift from static to dynamic infrastructure. However, to achieve ultimate success, organizations must align enterprise business outcomes such as productivity improvements, risk mitigation and cost optimization with key initiatives such as infrastructure modernization and faster application workload delivery.



HashiCorp's tools enable organizations to first unlock the journey and deliver a control plane for each layer across the cloud, including core infrastructure, security, networking, and application service delivery. By incorporating these tools into the key initiatives, significant business outcomes can be achieved. These outcomes include:

- Higher productivity gains of up to 80% due to consistent, automated workflows used across all teams and codified workflows that make debugging and issue resolution minimal.
- Cost savings of between 30-40% in cloud spend by using HashiCorp tools to understand the state of infrastructure and services at all times, making decisions about what can be deprovisioned or consolidated, or enforcing operational best practices within the workflow.

- Reduced risk around breaches occurring and providing organizations a holistic strategy to secure their applications and infrastructure while providing the means of quickly mitigating.

These business outcomes enable enterprises to succeed with cloud adoption and leverage HashiCorp products to implement a cloud operating model for digital transformation.

Case Studies

criteo

athenahealth

TMX

ROBLOX

Adobe

pandora

About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco and backed by Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP, and Bessemer Venture Partners. For more information, visit **www.hashicorp.com** or follow HashiCorp on Twitter **@HashiCorp**.

HashiCorp

www.hashicorp.com