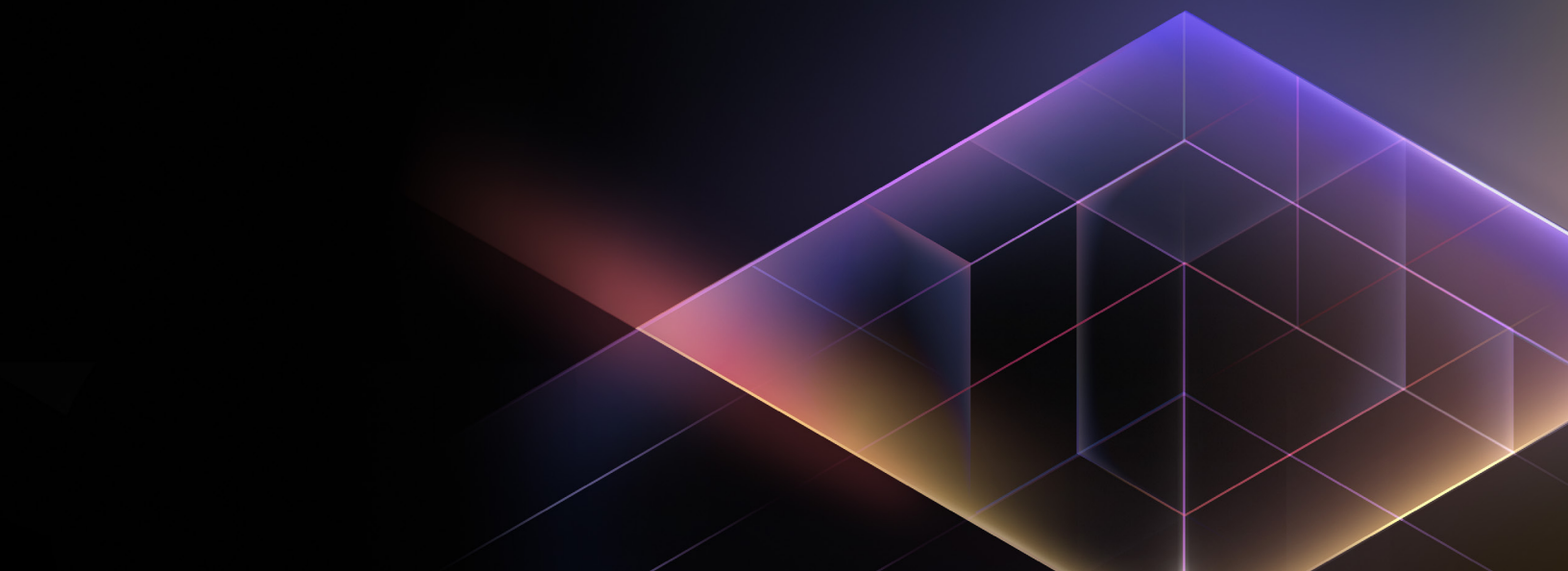
HashiCorp
an IBM Company

WHITE PAPER

The next generation of cloud security: Unified risk management, compliance, and zero trust

How to eliminate fragmentation, reduce risk, and enforce compliance in hybrid cloud environments



Introduction

Organizations are accelerating cloud adoption to improve the agility, scalability, and efficiency of their digital transformation initiatives. But the journey to the cloud — especially across hybrid and multi-cloud environments — isn't just about moving faster. It's about doing so without increasing risk and truly strengthening security and governance .

Compared to traditional IT, cloud infrastructure is dynamic, decentralized, and constantly evolving. Security models built for static, perimeter-bound networks can't keep up. In fact, they often get in the way — leading to fragmented tooling, inconsistent policies, and gaps attackers are quick to exploit.

This is the moment technical leaders are stepping into. As pressure mounts to deliver faster, they must also shield their organizations from risk and ensure regulatory alignment. The stakes are high, but so is the opportunity.

The Infrastructure Cloud from HashiCorp offers a new approach, a unified control plane that integrates Infrastructure Lifecycle Management and Security Lifecycle Management to enable proactive risk management, an enhanced compliance posture, and advanced zero trust cloud practices.

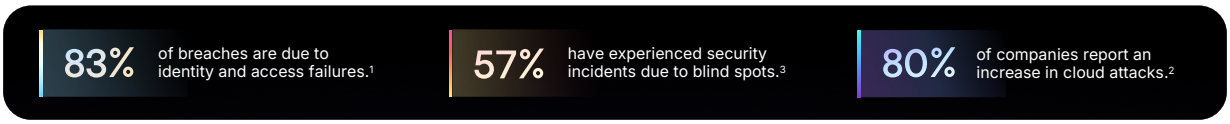
Table of Contents

The cloud security challenge: Expanding attack surfaces and compliance Complexity

As hybrid cloud adoption and AI scales, so do the challenges. Attack surfaces grow. Manual processes fail. And compliance becomes a game of catch-up. The journey from experimentation to maturity in hybrid cloud often results in silos, snowflake deployments, and an expanding attack surface that legacy tools cannot contain.

Too many organizations are stuck with fragmented security tools, disconnected workflows, and manual ticketing systems that can't keep up. Visibility is limited. Misconfigurations go unnoticed. And credentials live in too many places for too long. This isn't about theoretical risk. These are day-to-day operational failures that introduce gaps attackers can exploit.

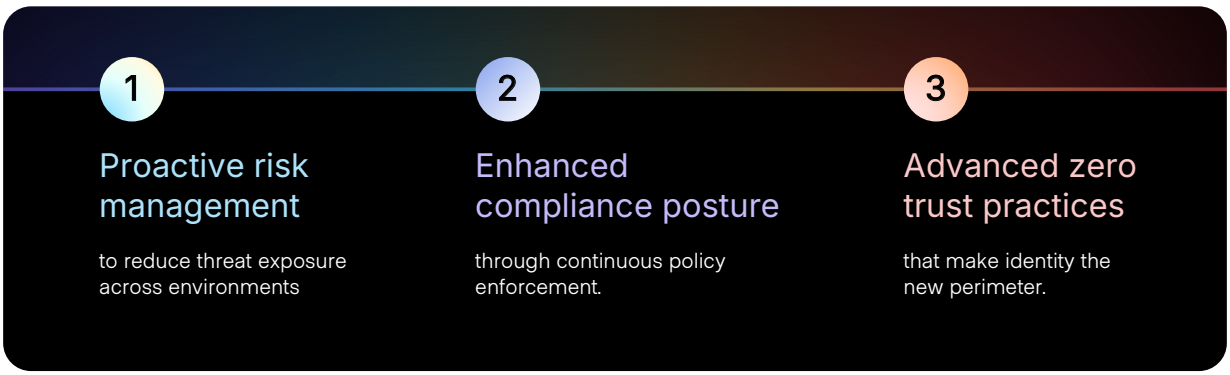
Consider this:



To fix this, organizations need more than better monitoring. They need a shift in how infrastructure is built, deployed and managed that's interwoven with security solutions that can protect, inspect, and govern your secrets, users, and services.

This shift is essential for today's technology leaders — who are being asked to move faster while maintaining tighter controls across environments. Strengthening security and governance isn't just a feature of modernization. It's the framework that makes modern cloud operations sustainable.

The following sections explore the three foundational capabilities that make this transformation possible:



Proactive risk management: Reducing threat exposure in hybrid cloud environments

The value of proactively addressing risk is clear, it's always much better to avoid security issues before they occur. But actually doing it — consistently, across every cloud and environment — is where most teams struggle due a lack of centralized control across environments.

Without centralized control and policy enforcement, cracks in the security processes begin to appear. Misconfigurations creep in. Unpatched vulnerabilities linger. Access controls drift. Over time, these gaps become systemic and spread throughout the digital estate, greatly expanding the attack surface.

The Infrastructure Cloud from HashiCorp empowers technical leaders to shift from one-off remediations to a repeatable, automated model that can:

- **Gain security insights from across the digital estate** using the centralized control plane provided by Terraform to review the health of your organization, detect security risks, and ensure policy enforcement across hybrid cloud environments.
- **Automate secrets and identity management** to eliminate the risk of shared credentials and overly broad permissions, by providing time-bound and least-privileged access to sensitive systems using Terraform, Vault, and Boundary.
- **Monitor and manage human and machine access** with active session monitoring, policy enforcement, and automated audit logging from Vault and Boundary.
- **Identify, prioritize, and remediate vulnerabilities** through streamlined remediation workflows and automated CI/CD pipelines across all environments using Terraform, Packer, and Vault.

At ManTech, for example, the security team knew long-lived credentials and inconsistent access controls posed a serious risk. **By adopting Vault to manage secrets and Boundary to standardize user access, they automated credential rotation and eliminated the need for local credential storage.** Their developers now work within a secure, policy-driven infrastructure built on Terraform workflows.

With risk under control, the next step in the journey of strengthening security and governance is ensuring that infrastructure adheres to the rigorous standards set by both internal stakeholders and external regulators.

Enhanced compliance posture: Governance at scale

Compliance isn't just a checklist — it's a business enabler. At their core, compliance regulations are designed to reduce risk for the businesses and customers. When done correctly they should align with business priorities. Yet 61% of enterprises cite compliance as a top cloud adoption barrier.[4]

For many teams, audits are still painful. Policies are inconsistently applied. And with regulations like SOC 2, PCI-DSS, HIPAA, and DORA all in play, the complexity is real. Risk and compliance teams often find themselves playing catch-up — interpreting regulations across regions, industries, and departments.

What these teams really want is clarity. They want to confirm, with confidence, that the infrastructure being deployed aligns with internal policy and external mandates. And they want to know this before an audit or breach.

That's why policy as code and continuous monitoring through a single system of record is so powerful. With policy as code teams can define, deploy, and enforce compliance policy consistently across the entire environment. It doesn't just reduce audit overhead — it builds trust across teams. **The Infrastructure Cloud provides the security and compliance teams a shared, automated foundation for demonstrating compliance without slowing down innovation.**

> "We knew that to succeed we'd need policy as code. We needed a paradigm shift that allowed full autonomy."
>
> **Jeremy Crawford**
> Head of Cloud Product, Deutsche Bank

Deutsche Bank

HashiCorp Terraform

The platform team at Deutsche Bank recognized the need for a common policy as code platform as they accelerated their operations. **With Terraform, they were able to build a library of compliant Terraform infrastructure modules and share them across the organization.** These pre-approved modules are backed by standardized financial regulation-related policies, so every deployment within the cloud platform team's workflow is compliant. Terraform also

provided a policy as code platform: Sentinel. This enabled automated policy checks on each Terraform deployment according to the cloud platform team's centralized policy framework.

The Infrastructure Cloud empowers compliance and risk teams to enforce consistent governance both pre and post deployment with:

- **A single system of record** and centralized control plane from Terraform and Vault ensures compliance before, during and after deployment.
- **Golden images and modules** standardize secure infrastructure and embed guardrails directly into CI/CD pipelines using policy as code.
- **Active user and session monitoring** identifies policy violations in real-time and flags drift from pre-approved configurations.
- **Streamlined compliance audits** are enabled through automated logging, secrets activity tracking, and session recording.

With governance and compliance woven into daily operations, the final piece of the transformation is about protecting what matters most: access. It's here that Zero Trust comes to life — not as a framework on paper, but as an operational reality rooted in identity.

Advanced zero trust practices: Identity-based cloud security

Many organizations today have an illusion of control. They assume that access is controlled, credentials are secure, and the right people have the right privileges. But in hybrid and multi-cloud environments where security is threatened by plaintext credentials buried in GitHub repos, VPNs that grant blanket access, or policies that aren't uniformly enforced, that illusion can break down quickly.

Zero trust is the only way forward. And with 80% of data breaches stemming from privileged misuse, identity-based security must be non-negotiable.[5] And yet, implementing it at scale is challenging without automation, visibility, and identity as the foundation.

HashiCorp addresses these challenges by helping organizations move from assumptions to assurances. With The Infrastructure Cloud, teams can secure access dynamically, without relying on brittle, perimeter-based models.

"Vault has proven to be a great equalizer for us, helping find the balance between ensuring the security and protection of our sensitive data and minimizing the amount of time and effort it takes."

Ganapathysaran Nambirajan
Senior Engineering Manager,
Platform Services, athenahealth

athenahealth

HashiCorp Vault

At athenahealth, this shift was transformative. Vault now handles over 3 million secrets requests per day, eliminating manual ticketing systems and reducing resolution time from four hours to under thirty minutes. **Zero trust is no longer a project — it's the way they operate.**

The key to success is leveraging identity-based access controls that can connect machines, people, and networks using trusted identities. Pairing identity-based access controls with advanced data protection can ensure organizations are protected from a proactive and reactive perspective. A comprehensive zero trust security architecture should include:

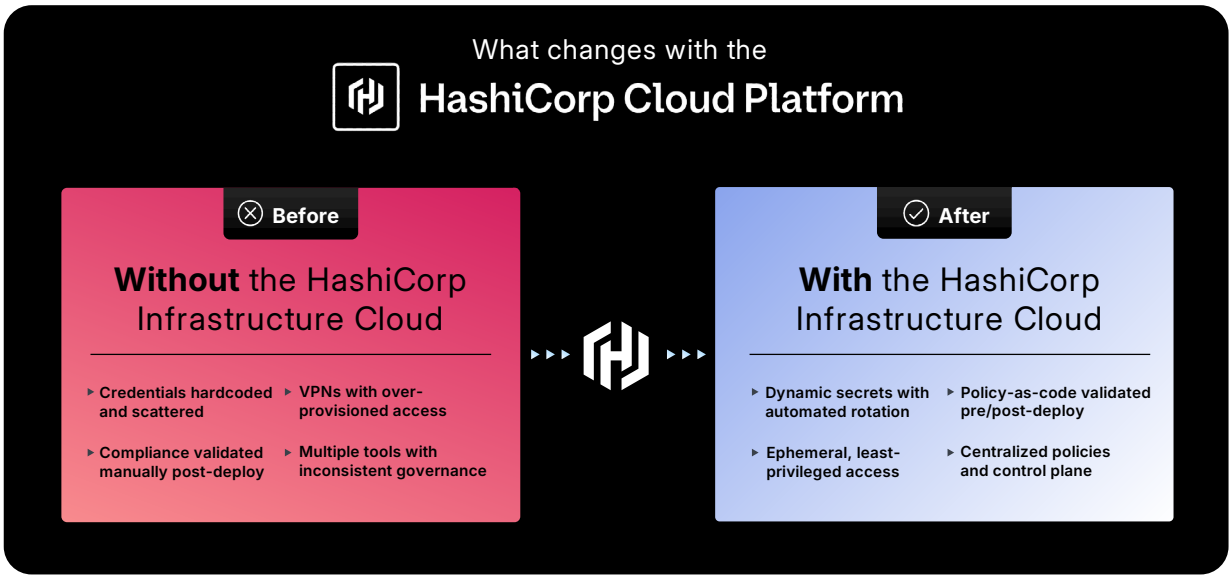
- **Secure human access with least-privileged and MFA controls** provides developers and operators with scoped, time-bound access to systems without relying on shared credentials or overly broad permissions.
- **Authentication of machine-to-machine access requests** reduces risk and standardizes secrets lifecycle management for machine identities.
- **On-Demand generation, rotation, and revocation of secrets** enforces secrets policies, reduces the risk of exposed secrets, and eliminates long-standing secrets.
- **Automatic and dynamic creation of keys and certificates** based on identity-based controls for both human users and machine-to-machine connections.

Together, these three capabilities form a cohesive security architecture — one that evolves with your organization, scales across environments, and aligns to the way teams actually build and deploy today.

Conclusion: Strengthen security and governance with The Infrastructure Cloud from HashiCorp

Doing cloud right means doing security right — and that starts with a unified strategy. The HashiCorp Infrastructure Cloud offers a blueprint that integrates Infrastructure Lifecycle Management (ILM) and Security Lifecycle Management (SLM) to deliver control, consistency, and scalability across every environment.

Whether it's reducing time to remediate, proving compliance in real-time, or accelerating developer workflows, the Infrastructure Cloud is built for this moment.



The path forward isn't piecemeal. It's integrated. The HashiCorp Infrastructure Cloud helps you eliminate risk, reduce manual work, and deliver secure, compliant infrastructure from day one. For technical leaders, this is the transformation you've been waiting for — and the partner that gets you there.

1. 2024 Verizon Data Breach Investigations Report
2. 2024 Crowdstrike Global Threat Report
3. 2024 IDC Cloud Security Survey
4. 2025 State of Cloud Security Report, Cybersecurity Insiders
5. 2020 Verizon Data Breach Investigations Report

About HashiCorp

HashiCorp is The Infrastructure Cloud™ Company, helping organizations automate multi-cloud and hybrid environments with Infrastructure Lifecycle Management (ILM) and Security Lifecycle Management (SLM). HashiCorp offers The Infrastructure Cloud on the HashiCorp Cloud Platform (HCP) for managed cloud services, as well as self-hosted enterprise offerings and community source-available products. The company is headquartered in San Francisco, California.

For more information visit hashicorp.com.