HashiCorp
an IBM Company

Secure by design: How to reduce cloud risk and maintain compliance

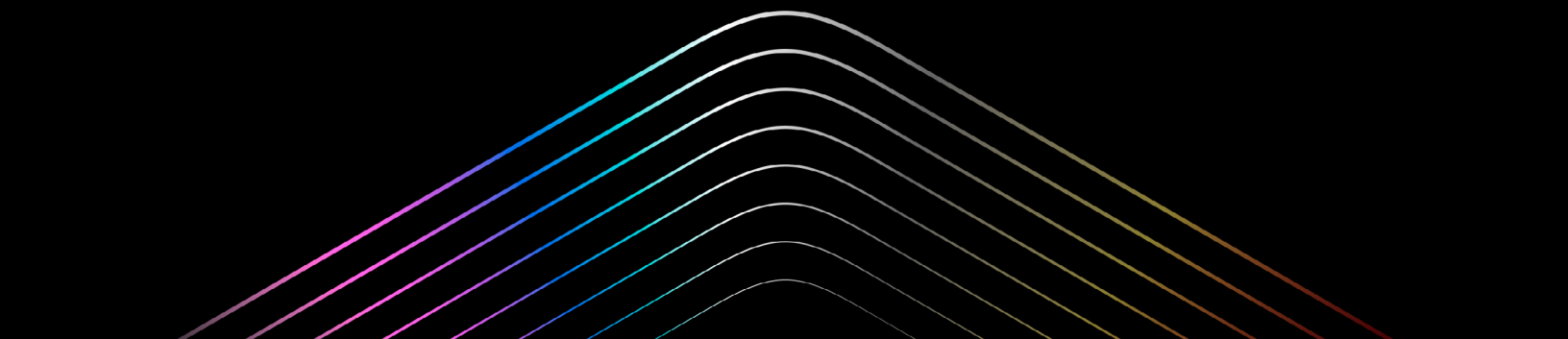
Security is not just an IT challenge; it's a boardroom priority.



Executive summary

With 98% of enterprises experiencing at least one cloud-related security incident, and compliance violations costing millions in penalties, the cost of getting it wrong is too high. However, as organizations expand into multi-cloud, complexity creates gaps that attackers exploit.

Leaders must answer a critical question: Can they scale their cloud infrastructure without introducing security and compliance gaps that expose the company to regulatory penalties and financial losses? This guide outlines how organizations can ensure security and governance at every stage of their cloud journey.



Multi-cloud security challenges

The cloud is a business necessity, and eight out of ten enterprises today use multiple cloud providers. As cloud environments grow and expand, they become more complex, and organizations face increasing vulnerabilities from a larger attack surface, fragmented visibility, and governance complexity.

Managing security in multi-cloud environments is complicated, and many organizations struggle with it. Seventy-five percent of companies have suffered security breaches from cloud misconfigurations, and nearly every organization (98%) has experienced at least one cloud-related security incident.

The problem is not typically on the provider end. Analysts agree Tier 1 cloud service providers deliver world-class security.[1] More often, the trouble is with the user. Gartner® even issued a strategic planning assumption saying, "Through 2027, 99% of records compromised in cloud environments will be the result of user misconfigurations and account compromise, not the result of an issue with the cloud provider."[2] Unlike fragmented security solutions that require different policies per cloud, HashiCorp's Infrastructure Cloud provides a unified control plane for security and compliance across all environments, reducing risk from misconfigurations before they happen.

For business leaders to reduce risk, they must strengthen security controls and enforce policies consistently across their cloud environments — public, on-premises, and hybrid — without dampening developer and IT productivity, which is easy to grasp in theory, but much more challenging to carry out.

81%

of enterprises use multiple cloud providers, which is complicating infrastructure management[3]

75%

of companies have suffered security breaches from cloud misconfigurations[4]

98%

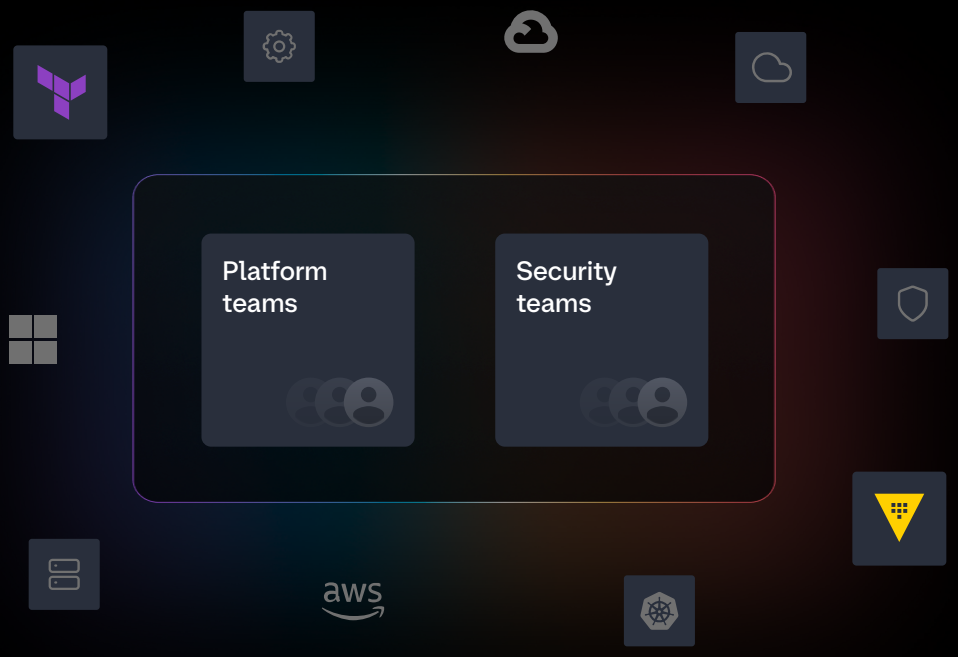
of companies have experienced at least one cloud-related security incident[5]

1. Gartner®: https://www.gartner.com/en/cybersecurity/topics/cloud-security
2. Charlie Winckless, Paul Proctor, Manuel Acosta, "Outcome-Driven Metrics You Can Use to Evaluate Cloud Security Controls," Gartner®, September 28, 2023.
3. Gartner®, Cloud Survey: Multicloud Adoption Remains the Norm, Michael Warrilow, February 26, 2024.
4. IDC Survey
5. **Cloud and AI Business Survey**: PwC

The reality for security teams

The responsibility of securing your multi-cloud estate falls to platform and security teams. For them to do their job, they are forced to deal with some harsh facts. Cloud-native tools provide limited visibility, preventing team members from seeing across cloud providers. As a result, they must learn to work with different security tools and configurations and manage separate systems for logging, alerts, access controls, encryption, and compliance.

To complicate matters further, modern, ephemeral cloud infrastructure is incredibly complex, and cloud-native security isn't up to the task. Regulations often change. And many organizations manually provision new cloud resources for speed and convenience, without enforcing clear boundaries.



Operating in a fragmented environment leads to vulnerabilities

Business leaders want to modernize their organizations and this means embracing modern cloud infrastructure. Complexity, lack of visibility, and inconsistent policy enforcement, however, make it difficult for their platform and security teams to manage security and compliance at scale.

Blind spots	Lack of visibility across cloud providers can result in security gaps, creating vulnerabilities for bad actors to exploit.
Misconfigurations	Lack of standardized controls increases the risk of configuration problems.
Inconsistent governance	Inconsistent enforcement of security policies across cloud providers leads to compliance failures, security breaches, and operational slowdowns.
Accounty compromise	Poor secrets management increases the risk of unauthorized access to sensitive data.

Every leader knows poorly protected cloud environments can result in outages, data breaches, and regulatory fines, which can potentially cost millions in lost revenue and remediation expenses. However, there are steps you can take to mitigate these risks.

Standardize the provisioning process

One of the leading causes of security breaches in the cloud is misconfigurations. Misconfigurations can happen for a variety of reasons, including:

- Someone unknowingly makes a mistake
- Teams don't understand the differences between cloud providers
- There is a lack of experience using different cloud-native security controls and tools
- Firewall rules are not properly set
- Failure to include security controls during infrastructure provisioning

Industry experts agree that the best way to avoid misconfigurations in the cloud is to standardize and automate infrastructure provisioning. By standardizing and automating this process, organizations overcome lack of consistency, which often accompanies manual efforts, and ensure security controls and policies are not overlooked or improperly set.

Many organizations accomplish this by using infrastructure as code and policy as code. This enables platform and security teams to build, deploy, and manage validated, pre-approved infrastructure. Whenever a new cloud environment is needed, developers can select a script, execute it, and the environment is built for them, with all required configuration settings and security controls included. This eliminates the risk of human error and ensures all policies are applied in compliance with organizational requirements.

Organizations that fail to standardize infrastructure provisioning are more likely to suffer security breaches due to misconfigurations. Don't wait for an incident — make security automation a priority today.

Enhance compliance posture through strong governance

Given all the differences between cloud providers, maintaining consistent governance in a multi-cloud estate is a challenge. Yet, remaining compliant with regulations (and avoiding potential fines or loss of customer trust) cannot be done without effective governance.

Lack of standardization and fragmented visibility across cloud environments are two of the biggest causes of non-compliance. If platform and security teams cannot enforce policies consistently, then cloud environments are at risk of failing to meet regulations, especially as regulations change over time and differ by location.

Configuration drift — where a system's settings change from pre-defined parameters, often rendering the system non-compliant — is another risk factor in cloud environments. This typically happens when resources are long-living and not closely monitored. If not mitigated, these changes can create vulnerabilities, expose organizations to threats, and put compliance at risk.

Leading organizations use end-to-end secrets management, automation, and policy as code governance to mitigate these risks. These capabilities make it easier to keep up with ever-changing regulatory requirements and ensure policies are enforced by using pre-built resources, images, modules, and registries that are secure and compliant by default.

Continuous monitoring of cloud infrastructure allows these organizations to identify configuration drift and remediate vulnerabilities proactively, reducing the chance of failed compliance audits.

Structure operations for proactive risk mitigation

When it comes to operating your business in the cloud, threats are unavoidable. Bad actors are relentless, and they have bots and sophisticated AI tools at their disposal to help them exploit vulnerabilities. Managing risk in multi-cloud environments is a struggle for many organizations. Without visibility and control across all cloud platforms or standardized infrastructure provisioning, it's common for organizations to have security gaps or blind spots, which can be easily scanned for and then exploited.

Other areas often targeted for exploitation are credentials and secrets. Secrets are sensitive pieces of data — like passwords, tokens, encryption keys, and certificates — that enable users to access resources and allow applications to communicate. By compromising identities and secrets, bad actors can gain access to sensitive information, compromise data, or lock down access to applications, creating a serious business risk.

Centralize visibility and control

Organizations are mitigating these risks through centralized control planes for infrastructure and policy management. By centralizing these key functions, platform and security teams gain visibility across all cloud environments, continuously monitor for vulnerabilities and policy gaps, and consistently enforce governance.

Automate secrets management

Secrets are critical for security, especially in application-to-application and machine-to-machine communications. To reduce the risk of compromise, leading organizations like Canva use centralized secrets management.

Canva is a SaaS company for B2B and B2C clients. The business relies on numerous APIs, databases, and services that require secure management of access credentials. The company has a massive customer base (over 170 million monthly users) and needs to support millions of secret reads monthly. But secrets were spread across many different stores, which reduced visibility and required significant manual effort to manage. This increased security risks for the company and made scaling operations a challenge. By centralizing and automating secrets management, Canva eliminated secret sprawl, increased visibility, and minimized security risks.

Canva | Through automated secrets management, Canva

2M

Secures 2M builds per month

87.5%

Reduced secret provisioning processes by 87.5%

100%

Can tie 100% of secrets back to an owner

Automated secrets management allows security teams to generate, store, rotate, and audit secrets and control access to them. This mitigates a key attack vector by preventing old credentials from lingering too long and ensures all identities are authenticated and trusted with least-privilege access to sensitive data, including just-in-time (JIT) credentials.

Deploy identity-based access control and encryption

Along with misconfigurations, account compromise is one of the leading causes of data breaches. The old security mantra is 'trust nothing and authenticate everything'.

To mitigate this risk, organizations use identity-based controls, and generate, rotate, and revoke secrets on-demand for dynamic and ephemeral environments. This enables authentication of every human, machine-to-machine, application, and service request using fine-grained controls and least-privilege access.

Securing data is another key mitigation approach. Many organizations use functions such as transparent data encryption, format preservation, and data masking and tokenization to protect sensitive data across all cloud environments. This ensures both data at rest and in motion is kept secure and reduces the risk of theft.

Enable proactive threat detection

Organizations are leaning on centralization, automation, and access control to create a unified system of record for all their security tools. This helps platform and security teams detect threats by monitoring environments and scanning code repositories and privileged access sessions for problems, enabling them to prioritize and mitigate vulnerabilities before they are exploited.

Reduce complexity through a unified approach

Multi-cloud scaling and complexity are realities every growing company faces. Many organizations are moving to a unified approach to infrastructure and security lifecycle management to overcome the challenges associated with security and governance in multi-cloud environments.

The Infrastructure Cloud from HashiCorp



The Infrastructure Cloud eliminates complexity and uncertainty in multi-cloud environments, giving you control, consistency, and confidence. You can simplify infrastructure provisioning, ensure security controls and policies are always present and enforced, and monitor environments for compliance for your entire multi-cloud estate — all from one centralized, unified solution.

A unified approach to security and infrastructure isn't just about reducing risk — it's about making cloud work for your business. The Infrastructure Cloud ensures that security is built-in, not bolted on, so your organization can innovate with confidence, knowing that compliance and governance are enforced at every stage.

Benefits of The Infrastructure Cloud

- Automated and codified infrastructure provisioning eliminates manual work and reduces the risk of misconfigurations
- A single system of record for infrastructure and security across all cloud environments reduces complexity and risk of blind spots
- Consistent security policies for all cloud environments remove the risk of inconsistent policy enforcement and human error
- Automated vulnerability and patch management ensures vulnerabilities are identified and mitigated proactively across any infrastructure
- Identity-based access controls reduce risk and increase trust through automated dynamic secrets generation and rotation for human and machine-generated identities and least-privilege access to sensitive data
- Ensures all security requirements are met using pre-built images, modules, and registries that have been tested and validated for compliance
- Transparent encryption, format preservation, data masking and tokenization, and automated creation of dynamic keys and certifications keep sensitive data protected, reducing the risk of data loss and misuse
- Compliance is maintained using customized audit logging and continuous security monitoring across all environments
- Third-party integration allows the use of any trusted identity provider for authentication, SSO, MFA, and context-based access controls, providing flexibility and consistency to further reduce risk.

About HashiCorp

HashiCorp is The Infrastructure Cloud™ company, helping organizations automate multi-cloud and hybrid environments with Infrastructure Lifecycle Management and Security Lifecycle Management. 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**.

Get started

To learn more about how The Infrastructure Cloud can help you strengthen security and governance in your multi-cloud estate, visit **hashicorp.com/infrastructure-cloud**

