

# Embed zero trust into the hybrid cloud operating model

Automate zero trust across hybrid cloud, securing every identity with continuous compliance and policy enforcement.

## Your expanding attack surface requires a proactive approach

81%

of enterprises report using multiple cloud providers, which is complicating infrastructure management<sup>1</sup>

98%

of companies have experienced at least one cloud-related security incident.<sup>2</sup>

75%

of companies faced security breaches from cloud misconfigurations.<sup>3</sup>

HashiCorp operationalizes zero trust across hybrid cloud by automating secrets management, enforcing human and non-human identity-based access, and continuously governing data, reducing security risk at scale.

### Identity-based access controls

Replace perimeter-based standing privilege with least-privilege, identity-driven access for humans and non-human identities across any environment.

- **Just-in-time human access:** Provide access to critical systems with time-bound, least-privilege access by default.
- **Non-human identity access management:** Issue ephemeral, identity-bound secrets with automatic rotation and revocation.
- **Application and service authentication:** Authenticate and authorize service-to-service traffic with strong service identity and mTLS.
- **Policy as code guardrails:** Codify zero trust standards so identity-based access is enforced by default.

### Sensitive data protection

Discover, centralize, control, and protect the entire data lifecycle from creation to deployment to ongoing management.

- **Secrets system of record:** Centralize secrets, keys, and certificates; generate dynamic credentials to reduce exposure.
- **Unmanaged secrets discovery and remediation:** Continuously scan code for leaked or unmanaged credentials, and bring secrets under centralized governance.
- **Encryption-as-a-service and key management (PKI):** Provide consistent encryption and managed keys across hybrid environments with granular permissions.
- **Data lifecycle management and auditability:** Automate certificate lifecycles and maintain centralized logs to speed audits.

1. Gartner, Cloud Survey: Multicloud Adoption Remains the Norm, Michael Warrilow, February 26, 2024.

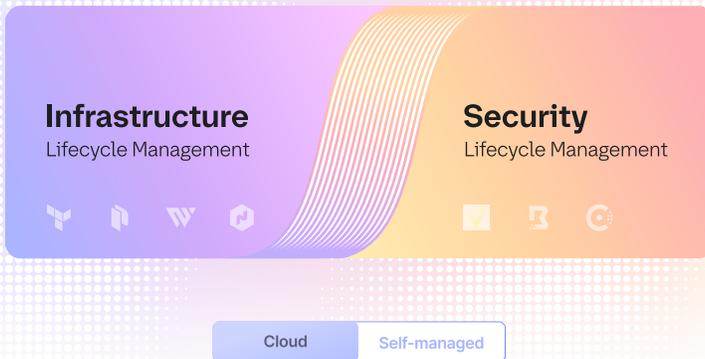
2. IDC Cloud Access Survey

3. [CrowdStrike's Insider's Playbook: Defending Against Cloud Threats](#)

## Secure innovation without compromise

HashiCorp empowers teams to innovate faster while ensuring security is never an afterthought. With centralized control, automated risk management, and policy-driven security, you can proactively reduce risk, simplify compliance, and strengthen governance across your entire digital estate.

### HashiCorp Cloud Platform



To learn more, contact your account representative or visit [www.hashicorp.com/en/infrastructure-cloud](https://www.hashicorp.com/en/infrastructure-cloud) to get started today.

### ManTech Systems Engineering Corporation

**“End-to-end security posture in line with our zero trust charter”**

Accelerated security setup and service delivery from 3 months to 3 weeks

[View study](#)



**“Credentials and secrets should be short-lived and subjected to fine-grained least privilege”**

Secured over 100,000 edge devices

[View study](#)

## Canva

**“Custom auth and secrets engines means the runway is unlimited”**

Secured 2 million monthly builds and backend secret reads

[View study](#)

© Copyright IBM Corporation 2026

IBM, the IBM logo, HashiCorp, and Vault 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](https://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.

It is the user's responsibility to verify the operation of any non-IBM products or programs with IBM products and programs. IBM is not responsible for non-IBM products and programs.

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.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

