HashiCorp
an IBM Company

An engineer's guide to saving time with proactive risk management

Mature risk management practices like centralized secrets management and identity-based access help organizations minimize threats and avoid the dreaded downtime they're associated with.

75%

Cloud security incidents that come from misconfigurations [1]

Addressing misconfigurations can prevent potential breaches and the associated costs.

292

Average number of days it takes to identify and contain a breach involving stolen credentials [2]

Using tools to identify unmanaged and rotate credentials can significantly reduce your likelihood of attack and save you time.

23%

MITRE ATT&CK tactics observed in cloud environments that involve credential access

Regularly rotating credentials and scanning for exposed secrets can help you stay secure and respond faster when threats arise.

The problem? Only 8% of organizations see themselves as highly cloud mature.

These organizations are more likely to have standardized on platform teams, leading to better management of cloud resources and reduced waste [3]

3 risk management practices to stay ahead

1.

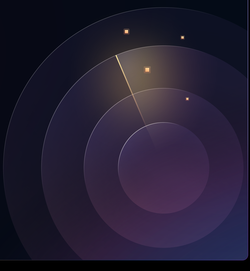
Centralize secrets management and detection

End-to-end secrets management helps protect applications, identities, and sensitive data.

Continuously monitor for unmanaged and leaked credentials using a secret scanner like HCP Vault Radar.

Establish a system of record to reduce overall security and system complexity.

Learn more: hashi.co/secret-scanning



2.

Adopt identity-based access controls

Secure connections between machines, people, and networks by seamlessly integrating trusted identities into your workflows.

Using a privileged access management solution like HashiCorp Boundary can get you started.

Learn more: hashi.co/identity-management

3.

Improve your compliance posture

Data leaks = financial loss, reputation hits, legal ramifications, and more.

Organizations that store sensitive, personal, and valuable data should use advanced data protection for:

- Encryption
- Tokenization
- Data transformations

Maintain governance and compliance across cloud environments. Infrastructure as code provides a good foundation for standardizing infrastructure across cloud environments.

Use policy as code to proactively test for compliant infrastructure configurations.

Give developers self-service modules to provision and manage infrastructure, which helps scale deployments across teams.

Learn more: hashi.co/policy-as-code

Learn more about taking a proactive approach to risk management in this on-demand webinar: hashi.co/riskdcr

1. Crowdstrike's Insider's Playbook: Defending Against Cloud Threats
2. IBM Cost of a Data Breach Report 2024
3. 2024 HashiCorp State of Cloud Strategy Survey

HashiCorp
an IBM Company