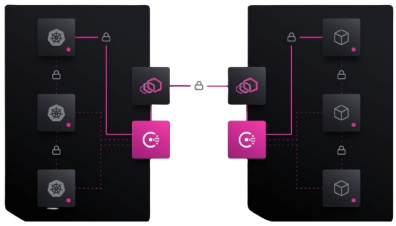
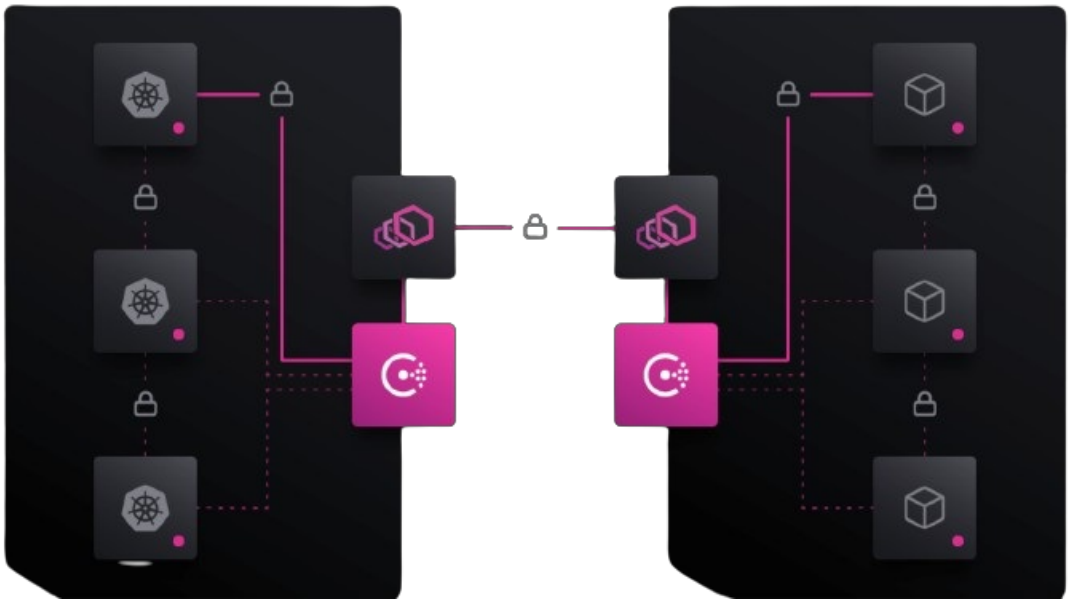


HashiCorp Zero Trust Security User Guide

HashiCorp Zero Trust Security



Contents

Trust Nothing

Authenticate and Authorize Everything.

The transition from traditional on-premises datacenters and environments to dynamic, cloud infrastructure is complex and introduces new challenges for enterprise security. There are more systems to manage, more endpoints to monitor, more networks to connect, and more people that need access. The potential for a breach increases significantly, and it is only a matter of time without the right security posture.

Securing traditional datacenters required managing and securing an IP-based perimeter with networks and firewalls, HSMs, SIEM, and other physical access restrictions. But those same solutions are no longer sufficient as companies move to cloud.

Securing infrastructure in the cloud requires a different approach.

As companies move to the cloud, the measures they took to secure their private datacenters start to disappear. IP-based perimeters and access are replaced by ephemeral IP addresses and a constantly changing workforce with the need to access shared resources.
Managing access and IPs at scale becomes brittle and complex.

Securing infrastructure, data, and access becomes increasingly difficult across clouds and on-premises datacenters, requiring lots of overhead and expertise. This shift requires a different approach to security, a different trust model. One that trusts nothing and authenticates and authorizes everything.

Because of the highly dynamic environment, organizations talk about a “zero trust” approach to cloud security. What does “zero trust” actually mean and what’s required for you to make it successful?

Challenges of multi-cloud zero trust security

Managing access by IPs

Traditional solutions for safeguarding infrastructure, data, and access are rooted in the need to secure based on IP addresses. Applications talking to databases, users accessing hosts and services, and servers talking across clouds — traditionally these have all been protected by allowing or restricting access based on IP addresses. Managing access to this same infrastructure and data as companies migrate to the cloud becomes significantly harder and operationally complex as IPs are more dynamic and change frequently.

Securing machine connectivity

Machine-to-machine access is a core element of a cloud-first organization. Legacy ITIL-based methods requiring conventional ticket systems are slow, burdensome, and not flexible enough to meet the rigorous security demands of today's dynamic cloud environments.

Scaling with demand

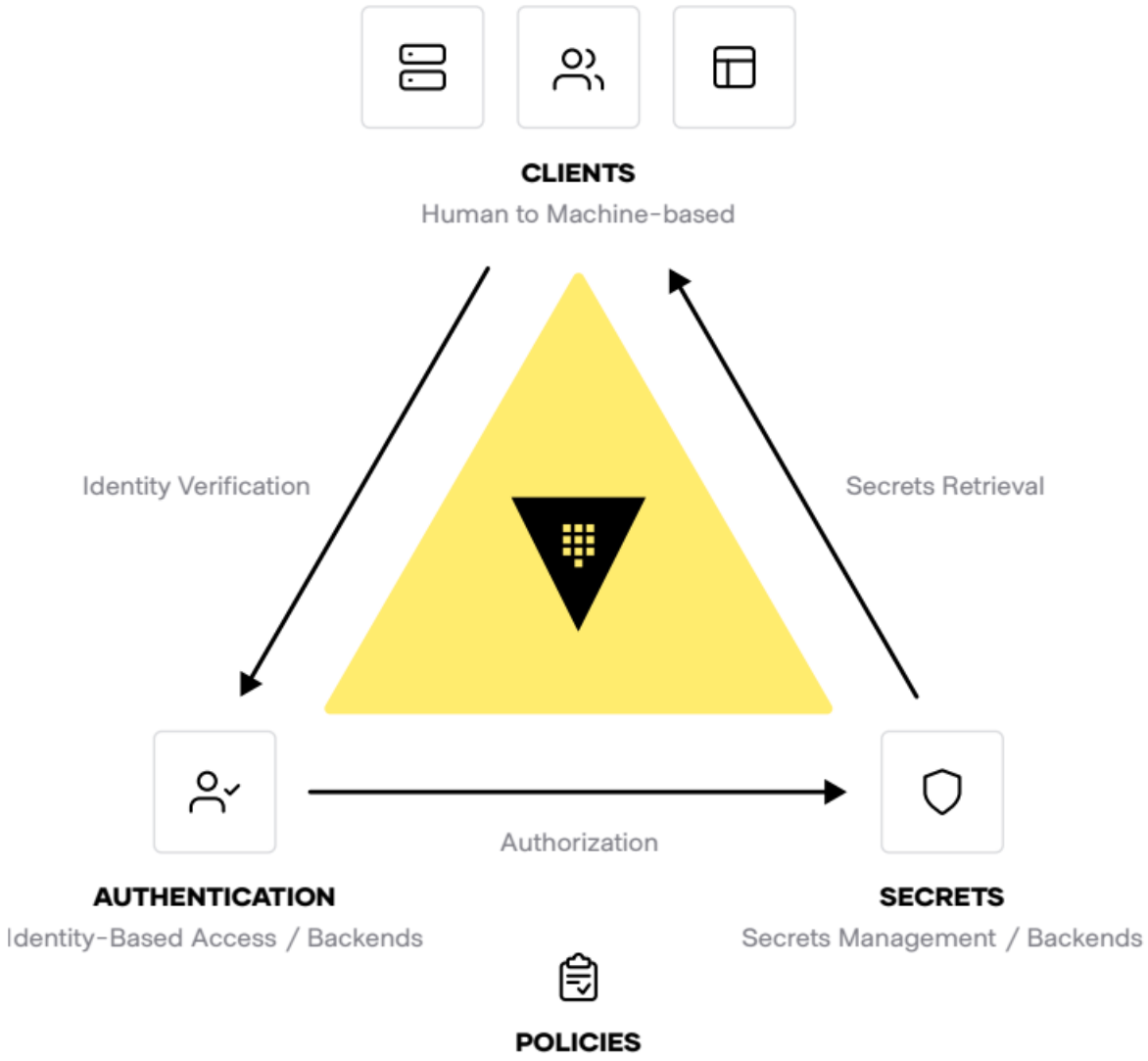
Traditional access and identity management with manual processes is slow, inefficient, and ineffective. Security measures like tokens, key cards, and passwords require direct IT intervention which requires significant resources and time, especially when required for hundreds or thousands of individual users and machines.

Enabling scalable, dynamic security across clouds

There are four pillars of multi-cloud security in a zero trust world:
machine authentication and authorization, machine-to-machine access, human authentication and authorization, and human-to machine access.
Across these four pillars is a consistent requirement: identity driven controls. 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.
Here's how the HashiCorp offerings can help you with each pillar and make zero trust security truly work:

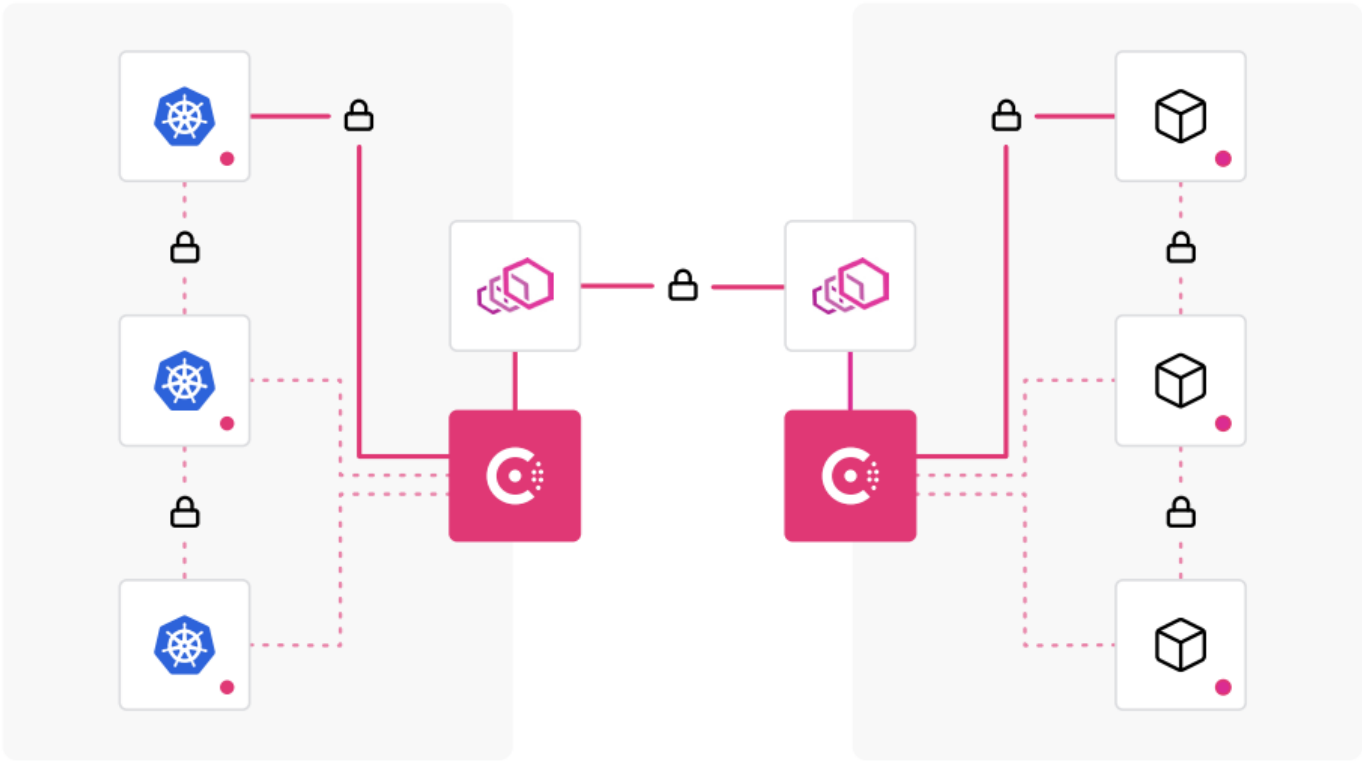
Machine Authentication & Authorization

HashiCorp Vault enables practitioners and enterprises to centrally secure, store, access and distribute dynamic secrets like tokens, passwords, certificates, and encryption keys across any public or private cloud environment. Vault provides an automated workflow for both people and machines to centrally manage access to credentials and encrypting sensitive data through a single API. With HCP Vault, get all of the power and security, without the complexity and overhead running it.



Machine-to-machine access

HashiCorp Consul enables machine-to-machine access by enforcing authentication between applications and ensuring only the right machines are talking to each other. Consul codifies authorization and traffic rules with encrypted traffic while automating identity-based access for maximum scale, efficiency, and security. With Consul, organizations can discover services, automate network configurations, and enable secure connectivity across any cloud or runtime using Consul service mesh.



Human access and authorization

Companies use different identity platforms for federated systems of record. Leveraging these trusted identity providers is the principle of identity-based access and security. HashiCorp products have deep integration with the leading identity providers.

Human-to-machine access

Traditional solutions for safeguarding user access used to require distributing and managing SSH keys, VPN credentials, and bastion hosts, which creates risks around credential sprawl and users having access to entire networks and systems. HashiCorp Boundary provides simple, secure remote access to securely access dynamic hosts and services without managing credentials, IPs, or exposing your network.

Business impact of multi-cloud security

HashiCorp approach to identity-based security and access provides a solid foundation for companies to safely migrate and secure their infrastructure, applications, and data as they move to a multi-cloud world.

Faster Cloud Adoption

Accelerate cloud adoption with push-button deployments and built-in best practices.

Increased Productivity

Increase productivity and reduce cost with fully managed infrastructure.

Multi-Cloud Flexibility

Enable multi-cloud flexibility with a single workflow for all providers.

Schedule your **free, personalized demo**.

CUSTOMER SUPPORT

www.hashicorp.com

Documents / Resources

	HashiCorp Zero Trust Security [pdf] User Guide Zero Trust Security, Zero, Trust Security, Security

References

- User Manual