

Guide to enabling zero trust security

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. Managing access and IPs at scale becomes brittle and complex.

Protecting infrastructure in the cloud requires a platform-based approach to [Security Lifecycle Management \(SLM\)](#).

As companies move to the cloud, IP-based perimeters and access are replaced by ephemeral IP addresses and a fast-moving workforce with the need to access shared resources in minutes, not days. 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 trust model; one that trusts nothing and authenticates and authorizes everything.

In highly dynamic distributed cloud environments, organizations talk about a “zero trust” approach to cloud security. What does “zero trust” actually mean and what’s required to adopt it successfully?

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.

Identity-driven controls enable multi-cloud zero trust security

Comprehensive SLM involves protecting secrets and certificates, inspecting your digital estate for unsecured credentials, and connecting only authorized machines, services, and people. The four pillars of zero trust cover most of those SLM components.

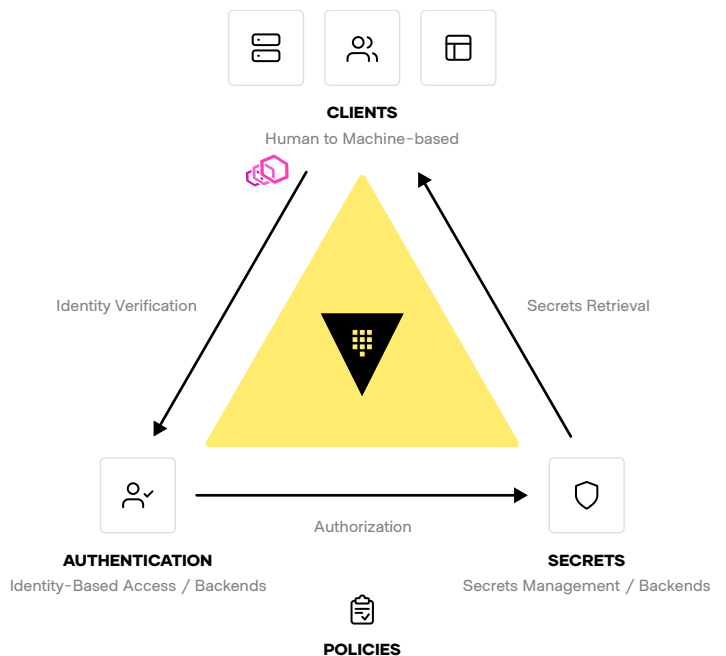
The four pillars of zero trust:

- Machine authentication and authorization
- Machine-to-machine access
- Human authentication and authorization
- Human-to-machine access

Across these four pillars is a consistent requirement: identity-driven controls. At HashiCorp, our SLM 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. Then the permissions attached to their identity 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 and authorization

[HashiCorp Vault](#) is the core identity broker many enterprises use to centrally store, access, and distribute dynamic secrets like tokens, passwords, certificates, and encryption keys across any hybrid or multi-cloud environment. Unlike burdensome ITIL-based systems, HashiCorp solutions issue short-lived credentials in a dynamic fashion, enabling fast and secure exchange of keys, credentials, certificates, and more between systems and applications.



Machine-to-machine access

[HashiCorp Consul](#) secures machine-to-machine access over the network by enforcing encryption and authentication between applications at microservice-scale, ensuring only authorized machines are talking to each other. Consul also takes the identity-based approach to codify and enforce traffic rules. With Consul, organizations can discover services, automate network configurations, and enable secure connectivity across any cloud or runtime using Consul [service mesh](#).

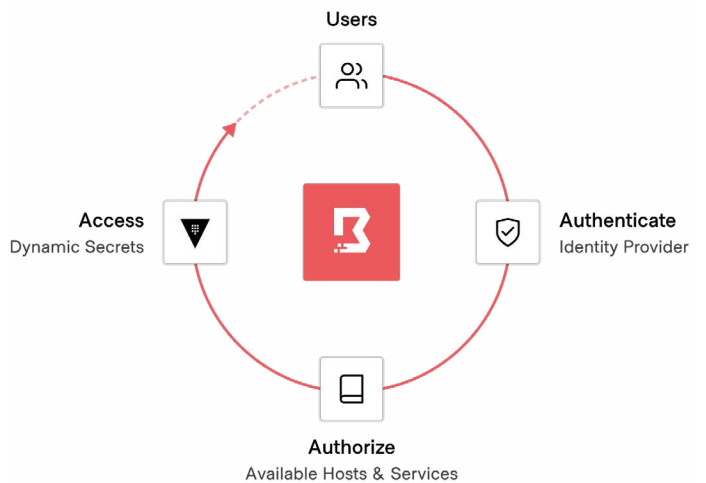
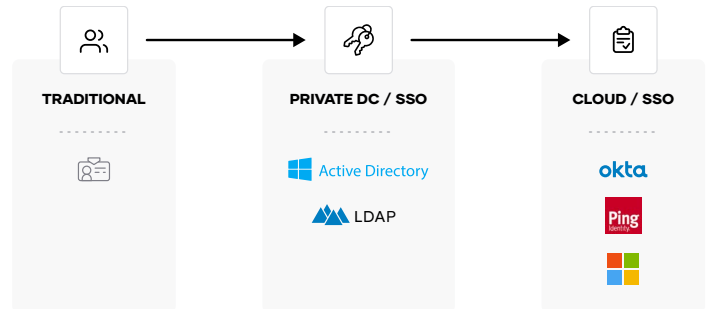
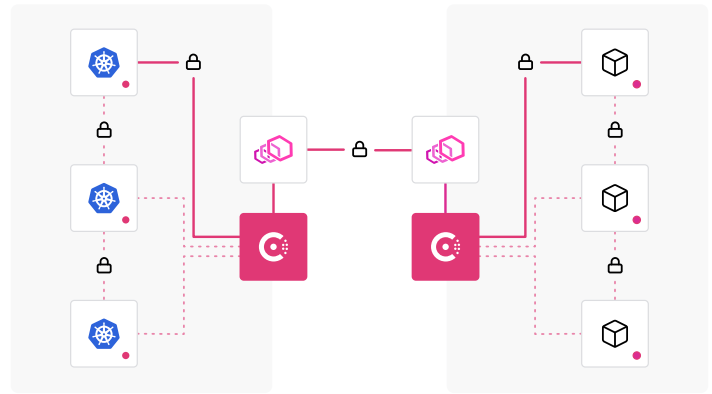
Human identity authentication

Companies use different identity platforms (IdPs) for federated systems of record. These could include Active Directory, LDAP, Okta, Ping, and many more. Leveraging these trusted identity providers supports 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 include network devices like VPNs or bastion hosts. This approach provides users with access to all resources on the network and does not enforce least-privilege access without requiring additional devices like network firewalls. This approach also does not help with credential management, requiring users, admins, or other tools to manage and distribute credentials like SSH keys, certificates, and username/password. This outdated approach to accessing infrastructure resources creates significant risks and management toil.

Enterprises often end up with [credential sprawl](#) and many times give users access to entire networks to cut through slow processes. [HashiCorp Boundary](#) is the modern way to do PAM that streamlines end-user access and improves security by enforcing least-privilege access. It provides smart layers of abstraction, automation, and security without exposing your network or requiring users to manage credentials. Boundary integrates with Vault to secure access to applications and critical systems with fine-grained, single-use authorization tokens, removing the need for manual credential generation and management.



Business impact of multi-cloud security

HashiCorp's 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 modern, centralized security platforms.



Multi-cloud flexibility

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

Learn more about enhancing multi-cloud security in a zero trust world by scheduling your [free, personalized demo](#).

© Copyright IBM Corporation 2025

Produced in the
United States of America
August 2025

IBM, the IBM logo, HashiCorp, Vault, Consul and Boundary 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.

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.

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.

