HashiCorp

Trust Nothing. Authenticate and Authorize Everything.

Enabling Zero Trust Security in the Public Sector

Introduction

The migration to cloud means teams and organizations must rethink how to secure their applications and infrastructure. Security in the cloud is being recast from static and IP-based – defined by a perimeter—to dynamic and identity-based—with no clear perimeter. Nowhere is this more true than in the public sector, where organizations are not just protecting their own data, but that of the people and constituents they are sworn to serve. This idea is known as **zero trust security.**

The recent Executive Order on Improving the Nation's Cybersecurity, from May 12, 2021 states that "The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals."

In accordance with this executive order, the Cybersecurity & Infrastructure Security Agency (CISA) has published the following definition of critical software that it deems as needing to conform to these larger zero trust security considerations and is thus subject to the further requirements of the executive order (EO).

EO-critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

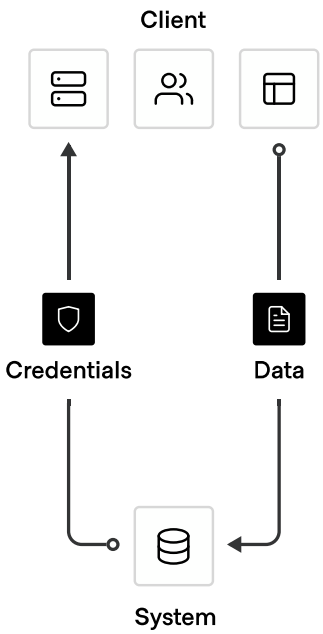
- Is designed to run with elevated privilege or manage privileges;
- Has direct or privileged access to networking or computing resources;
- Is designed to control access to data or operational technology;
- Performs a function critical to trust; or,
- Operates outside of normal trust boundaries with privileged access.

As a result, agencies that are mandated to leverage EO-critical software and systems need to fully understand and embrace zero trust security, then plan and execute an implementation strategy.

Cybersecurity Challenges of the Cloud

The transition from traditional on-premises datacenters and environments to dynamic, cloud infrastructure is complex and introduces new challenges for the security of public sector organizations. There are more systems to manage, more endpoints to monitor, more networks to connect, and more people that need access. This is especially true as public sector organizations adopt multi-cloud and hybrid cloud environments, increasing these challenges exponentially.

We expect this trend to continue as more and more agencies expand their cloud services through multiple vendors in order to increase flexibility and better fit their mission critical needs. A prime example of this can be seen with the CIA, which recently awarded its Commercial Cloud Enterprise (C2E) contract to five vendors: Amazon, Google, IBM, Microsoft, and Oracle. As this expansion continues, the potential for a breach increases significantly, and it is only a matter of time without the right cloud-agnostic security posture.



Securing traditional datacenters requires managing and securing an IP-based perimeter with networks and firewalls, hardware security modules (HSMs), security information event managment (SIEM), and other physical access restrictions. But those same solutions are no longer sufficient as organizations move to the cloud. Securing infrastructure in the cloud requires a different approach.

As the public sector moves to the cloud and updates its processes to conform to new federal mandates, the measures organizations previously took to secure their private datacenters become obsolete. IP-based perimeters and access are replaced by ephemeral IP addresses. In addition they now have 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 and 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 in practice and what's mission critical for you to make it successful?

What is Zero Trust Security?

Zero trust security is predicated on securing everything inside and outside of your systems based on trusted identities. Think of it like this: Instead of being let in the gate of a secure building and being allowed to wander freely, you are instead accompanied by a guard with a temporary ID issued at the gate that allows you into only certain areas. Even if a malicious actor gets through the front gate, they still encounter security checks at every area, verifying their ID with the guard standing watch.

Challenges of Multi-Cloud Zero Trust Security in the Public Sector

Public sector organizations face unique challenges as they attempt to complete this zero trust transformation. It's important to understand four of the main obstacles.

Managing access by IPs

Traditional solutions for safeguarding infrastructure, data, and access are rooted in the need to provide security 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.

Digital Shift and Remote Workforce

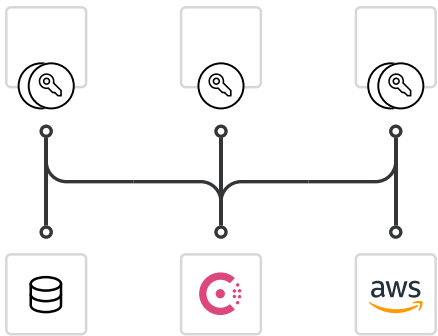
Organizations' digital transformation, both in terms of infrastructure and workforce, have contributed to increased data breaches and ransomware attacks to the public sector. This has been shown by numerous attacks including data breaches at the Census Bureau, Department of Veteran Affairs, and countless other public sector organizations. This is in addition to recent supply chain ransomware attacks. More than 35% of cybersecurity professionals polled by Deloitte cite these challenges as driving their zero trust adoption.

How to Implement a Zero Trust Security Posture

HashiCorp has outlined six steps organizations in the public sector should take to increase their zero trust security posture and reduce risk due to an attack or breach.

Step 1: Centrally Store and Protect Secrets/Credentials

A key challenge to organization security posture is secret sprawl. Secret sprawl is when you have key credentials, tokens, passwords, etc. littered all over your infrastructure.



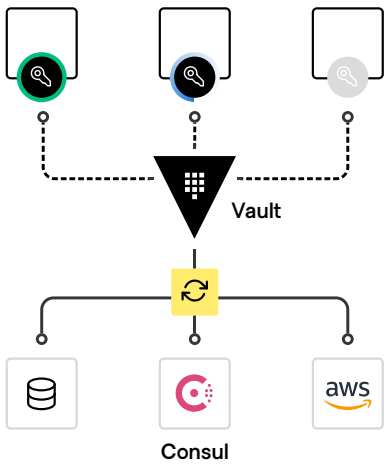
Consul

Many traditional IT departments have a database username and password that's hard-coded into the source code of an application. It's in plain text in the configuration file. It's in plain text in config management. It's in plain text in version control. It's in a Dropbox and it's in a Wiki. It's sprawled all over your infrastructure in different places and easily accessible to anyone who has access to any level of your systems.

Removing plaintext secrets stored in source code or saved on computers is a start. In order to be secure, organizations must secure, store, tightly control, and monitor access to tokens, passwords, certificates, and encryption keys for protecting secrets and other sensitive data.

Step 2: Leverage Dynamic Credentials

As companies move out of private datacenters, they're faced with new operational and security issues across their applications and infrastructure. As previously discussed, secrets, such as passwords, tokens, certificates, and encryption keys previously stored in on-premises systems now create vulnerabilities in source code as systems are moved into public repositories and cloud instances.



In addition to centrally storing, controlling, and monitoring access to tokens, passwords, certificates, API keys, and encryption keys that protect systems and sensitive data, organizations also need to leverage dynamic credentials to further increase their security. Oftentimes vulnerabilities occur due to weak or non-rotated secrets, allowing attackers to access protected data, often for long periods of time. By tightly coupling trusted identities with access, you can maintain a tighter security posture — rotating, updating, and revoking access through the use of dynamic secrets.

Dynamic secrets eliminate the ability for attackers to steal credentials as they don't exist until they are read. In addition, they can be automatically revoked immediately after use, minimizing the amount of potential damage by reducing the window of opportunity to use stolen secrets.

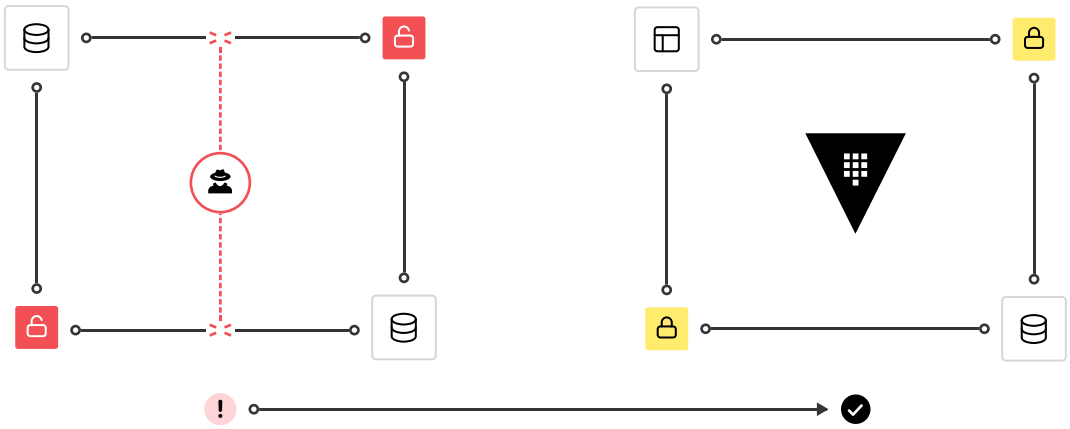
Step 3: Replace Perimeter-Based Security with Identity-Based Security

The transition from traditional on-premises datacenters and environments to dynamic, cloud infrastructure is complex and introduces new challenges for organizations security. There are more systems to manage, more endpoints to monitor, more networks to connect, and more people that need access. This greatly increases the potential for breaches, requiring action to secure your infastructure.

To solve this requires the introduction of identity-based security that focuses on access to digital information or services based on the authenticated identity of an individual or service. Such solutions tie access to a single identity, which, once verified, determines what networks, solutions, and data one is entitled to, ensuring they are accessing only what they should be able to. In addition, it becomes much easier to see who has access to what and then to adjust or revoke privileges as needed.

Step 4: Encrypt Everything

Organizations are used to encrypting full volumes of data, such as disks. But oftentimes breaches or a system being compromised is due to someone with access. Encrypting data in transit and at rest ensures that if a system is compromised, the encoded data remains safe.

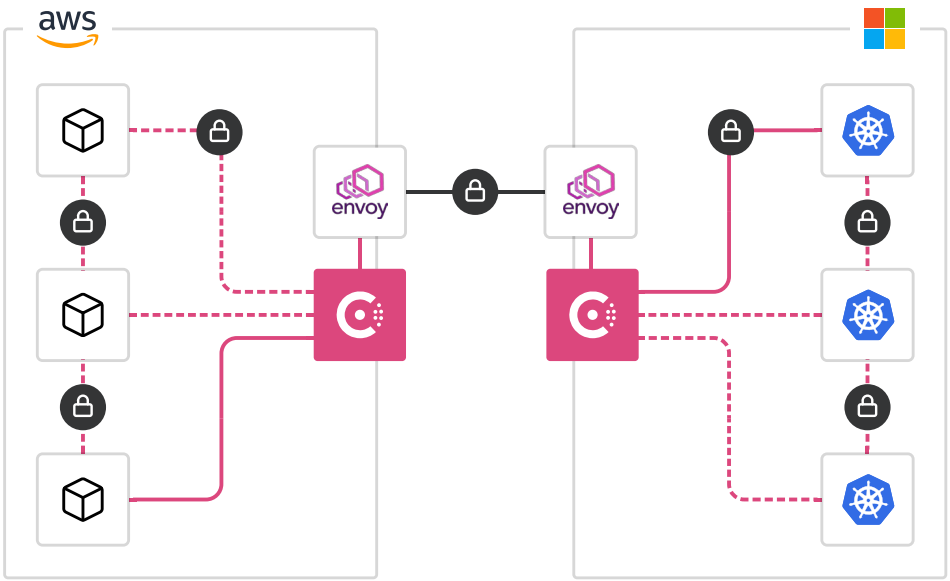


Prevention should always be the primary goal of any security solution, but prevention is often the last step companies take. Protecting and securing sensitive data as if you knew someone was already on the network creates a scenario where even if a breach were to occur, your most sensitive data or information is still safe.

Step 5: Authenticate and Authorize all Network Traffic

As we have already discussed, the move to the cloud leads to the measures previously taken to secure private datacenters start to disappear. Due to IP-based perimeters and access being replaced by ephemeral IP addresses, 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 trust model that trusts nothing and authenticates and authorizes everything. Machine-to-machine access is a core element of a cloud-first organization. Machine-to-machine access must enforce authentication between applications and ensure that only the right machines are talking to each other. This can be implemented through the use of a service mesh that creates a consistent platform for modern application networking and security with identity-based authorization, Layer 7 (L7) traffic management, and service-to-service encryption.



Step 6: Multi-Factor Authentication (MFA)

Protecting user accounts is vital to an organization's security strategy. Cyber criminals use legitimate credentials that have been compromised to gain a foothold in a network, avoiding detection for an average of 228 days in 2020 according to IBM. More than 60% of hacking-related breaches involved weak or compromised passwords, according to Verizon's 2021 Data Breach Investigations Report. Microsoft Security reports that enabling multi-factor authentication (MFA) reduces account credential compromises by 99.9%.

Identity-Driven Solutions for the Four Pillars of Zero Trust

The common thread through all six steps for implementing zero trust security is identity. Based on this, there are four foundational categories for identity-driven controls and zero trust security:

Identity Driven Controls

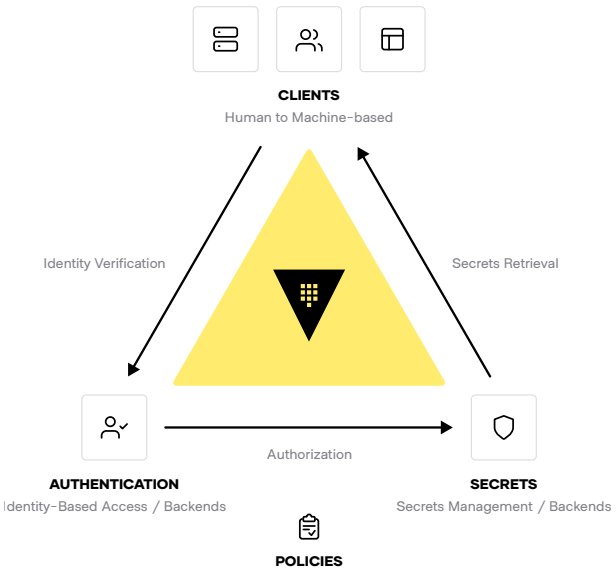
MACHINE AUTHENTICATION & AUTHORIZATION	MACHINE-TO-MACHINE ACCESS	HUMAN-TO-MACHINE ACCESS	HUMAN AUTHENTICATION & AUTHORIZATION

Identity-Driven Controls are a Requirement Across All Four Pillars of Zero Trust

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:

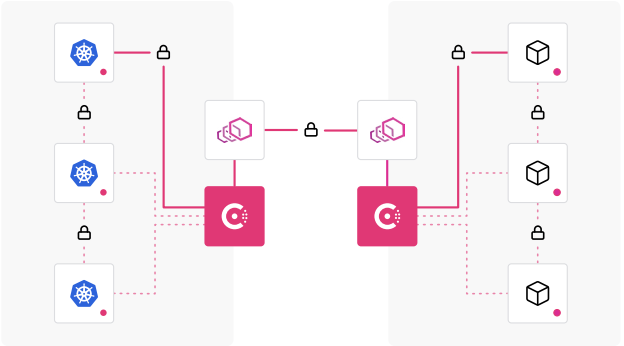
Machine Authentication & Authorization

HashiCorp Vault enables practitioners and organizations 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.



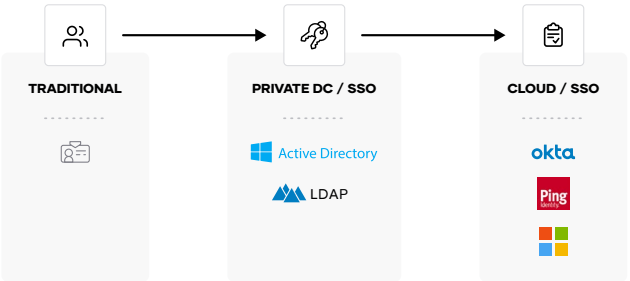
Machine-to-Machine Access

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.



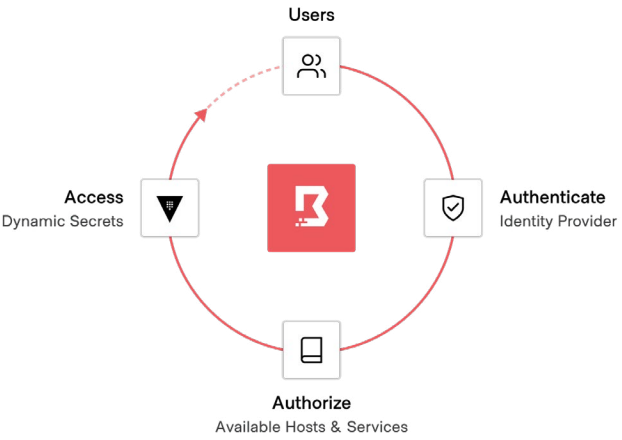
Human Access and Authorization

Public sector organizations use different identity platforms for federated systems of record. Leveraging these trusted identity providers is the key 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 or IPs, or exposing your network.



Public Sector Impact of Multi-Cloud Security

HashiCorp's approach to identity-based security and access provides a solid foundation for organizations to safely migrate and secure their infrastructure, applications, and data as they move to a multi-cloud world and adjust their security posture in order to conform to new EO-critical requirements.

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.

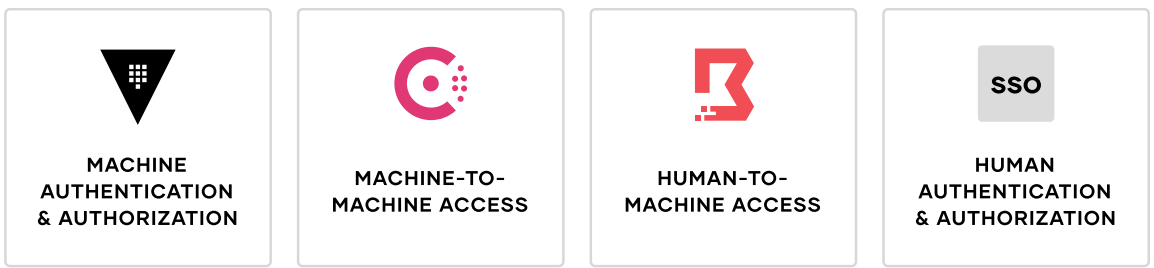
Multi-Cloud Flexibility

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

Multi-Cloud Security in a "Zero Trust" World

By following these steps and leveraging the HashiCorp security product stack to help standardize your security posture, public sector organizations will be in a strong position to protect themselves and comply with the security requirements that are quickly becoming mandatory.

Identity Driven Controls



To learn more about how HashiCorp can help you on this journey, please reach out to our public sector team here: hashicorpfederal@hashicorp.com

About HashiCorp

HashiCorp is the leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-data center functionality. The company is headquartered in San Francisco and backed by Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP, and Bessemer Venture Partners. For more information, visit www.hashicorp.com or follow HashiCorp on Twitter @HashiCorp.

www.hashicorp.com