

# Standardize identity-based secrets management

The standard for security automation to manage access to secrets and protect sensitive data

# Identity-based security has evolved with cloud

With the shift to cloud and hybrid infrastructure, companies no longer manage static IT estates with trusted perimeters. In modern dynamic environments, networks and IPs can't be trusted, and each application and user could pose a threat. That's why organizations are adopting identity-based security architectures built on the foundation of zero trust.





Datacenters with inherently high-trust networks with clear network perimeters.

### Traditional approach

- High trust networks
- · A clear network perimeter
- Security enforced by IP-ADDRESS

## Dynamic



Multiple clouds and private datacenters without a clear network perimeter.

### Vault approach

- · Low trust networks in public clouds
- · Unknown network perimeter across clouds
- Security enforced by application identity

# HashiCorp Vault

Secure, store and tightly control access to tokens, passwords, certificates, encryption keys, and other sensitive data using a UI, CLI, or HTTP API.

- · Centrally store, access, and distribute static & dynamic secrets
- Allows Kubernetes services to authenticate & request their own credentials
- Automated service account rotation
- · Protect data with centralized key management

STANDARDIZE SECRETS MANAGEMENT Certificates Data Protection Secrets Keys Static PKI KMS Encryption KMIP Dynamic Managed Keys Signatures HSM Tokenization Database Kubernetes Trillions+ 250M+ 70%+ Þ (1)8 of top 20 US banks Secrets Downloads managed/year

## Benefits

## 50% Less time spent

## Reduce risk of data exposure

Encrypt sensitive data in transit and at rest using centrally managed and secured encryption keys in Vault, all through a single workflow and API.

## 100K+ Edge devices supported

### Reduce the risk of a breach

Eliminate static, hard-coded credentials by centralizing secrets in Vault and tightly controlling access based on trusted identities.

## 0% Unplanned downtime

### Increase productivity

Enable development teams to automatically consume secrets in their application delivery process and protect sensitive data programmatically through a single API.

Supported technologies and identities							
	aws	4	Google Cloud	•÷	okta		
	cassandra	My <mark>SQL</mark> .	C-)	THALES	🗞 kafka	<b>1</b>	
		ORACLE <sup>®</sup>	MongoDB.	$\mathbf{O}$	DIIO	LDAP	
	splunk>	¢	<mark>Arc</mark> Sıght <b>∢</b>			<b>2</b>	
	<pre>@etcd</pre>	Pivotal.	Q	SQL Server	🊧 paloalto <sup>.</sup>		
Trusted by	Compare offerings				<b>Community</b> Individuals	<b>HCP</b> Teams	Enterprise Premium Organizations
	Adopt	Sec	ure storage		$\checkmark$	$\checkmark$	$\checkmark$
(9)	Service registry	, Vau	lt agent		$\checkmark$	$\checkmark$	$\checkmark$
Adobe	and discovery	Det	Detailed audit logs			$\checkmark$	$\checkmark$
		Nar	Namespaces			$\checkmark$	$\checkmark$
BARCLAYS 🕸			Silver support: 9x5 w/ SLA			$\checkmark$	$\checkmark$
	Gold support: 24/7 v			/ SLA		$\checkmark$	$\checkmark$
SAP Ariba							
<u>_</u>	Standardi	ze Cre	dential leasing & re	evocation	$\checkmark$	$\checkmark$	$\checkmark$
SPACEFLIGHT	Secure network	king Sec	Secure plugins			$\checkmark$	$\checkmark$
	Entities & entity groups			S	$\checkmark$	$\checkmark$	$\checkmark$
CIUISC	UI with cluster management				$\checkmark$	$\checkmark$	$\checkmark$
credit karma	Control groups Multi-factor authentication Read replicas Replication Benlication filters						$\checkmark$
CIECICKAITTA				ation		$\checkmark$	<i>~</i> ,
						$\checkmark$	$\checkmark$
							$\checkmark$
		nep	incation miters				$\checkmark$
	Scale	ACI	_governance & ten	nplating	$\checkmark$		$\checkmark$
	Governance	Enc	ryption as a service	9	$\checkmark$		$\checkmark$
	compliance an	<sup>d</sup> Key	rolling		$\checkmark$		$\checkmark$
	reliability	Disa	aster recovery (DR)				$\checkmark$
		Aut	o-unseal AWS KM	S		$\checkmark$	$\checkmark$
		Aut	o-unseal GCP Clou	ud KMS			$\checkmark$
		Aut	o-unseal Azure Ke	y Vault		$\checkmark$	$\checkmark$
		Sen	tinel policy as code	e management		$\checkmark$	$\checkmark$
		HM	S Auto-unseal				$\checkmark$
		FIPS	S 140-2 & cryptog	enic compliance	e		$\checkmark$
. <u> </u>							

HashiCorp www.hashicorp.com