
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT239

SPONSORED BY HASHICORP

Zero Trust security with HashiCorp Vault and AWS

Andrew Manoske (he/him)

Principal Product Manager – Crypto and Security Products
HashiCorp

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.


COMCAST
SAMSUNG
SEAT GEEK
gm
shopify
Booking.com
ADT
wepay
a CHASE company
Lufthansa
co-operators
cruise
Blackstone
STANDARD &POOR'S
GENSCAPE
Santander
PROGRESSIVE
Grab
pivotree
criteo
NBCUniversal
AstraZeneca
TRACTOR SUPPLY Co
BARCLAYS
BNP PARIBAS
agl
vodafone
ARUP
Lincoln Financial Group
H&R BLOCK
AIRBUS
athenahealth
ABN·AMRO
SAP Ariba
FERGUSON
Kansas City
DAZN
YOOX NET-A-PORTER GROUP
WARE2GO
Loblaw Companies Limited
USVenture
THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC
ROBLOX
GoodRx
UBISOFT
sky
surescripts
Q2
priceline.com
KPMG
Nationwide
gsk
AXA
RED VENTURES
BHP
DECATHLON
Shipt
OLD DOMINION FREIGHT LINE
nab
Anaplan
cielo
AUTODESK
sumup
ellume
AirPlus INTERNATIONAL
KeyBank
Qlik
VINGROUP
2K
ADB
CREDICORP
olo



Modern Infrastructure

- No trusted perimeter
- No trusted access
- Unsecured data

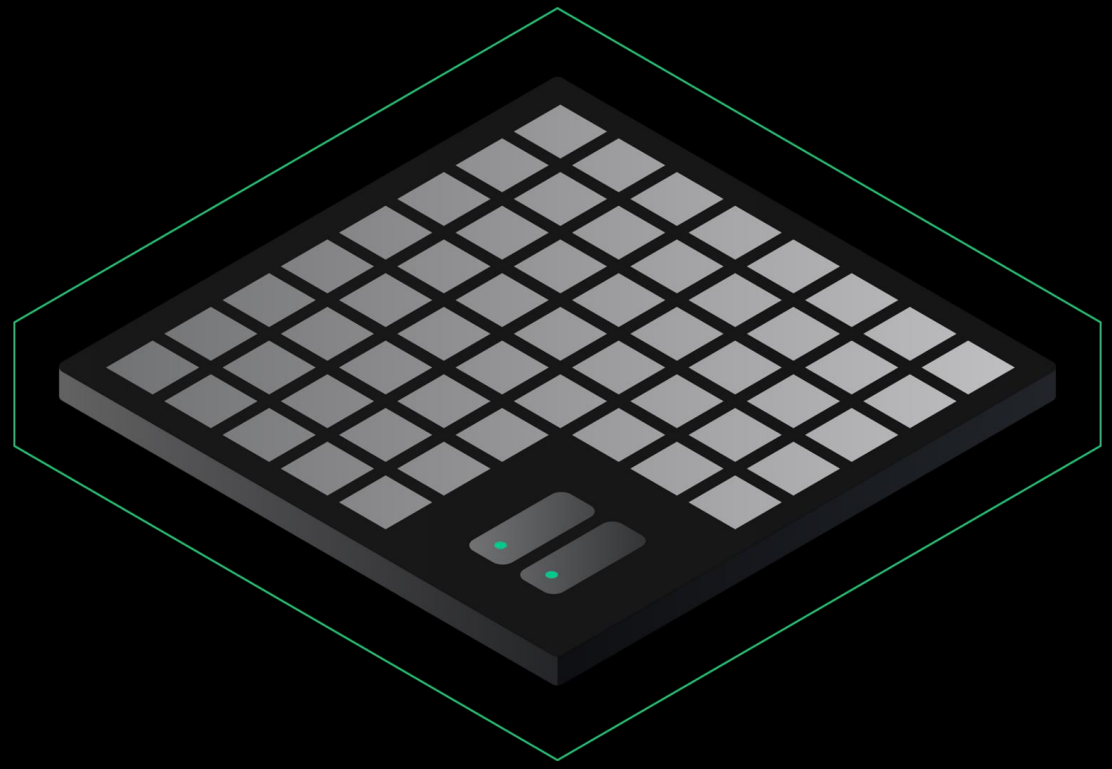


Modern Infrastructure

*with **HashiCorp Zero Trust Security***

- Everything is authenticated
- Every action is authorized
- Data is always protected

Securing a Data Center Used to Seem Simple.

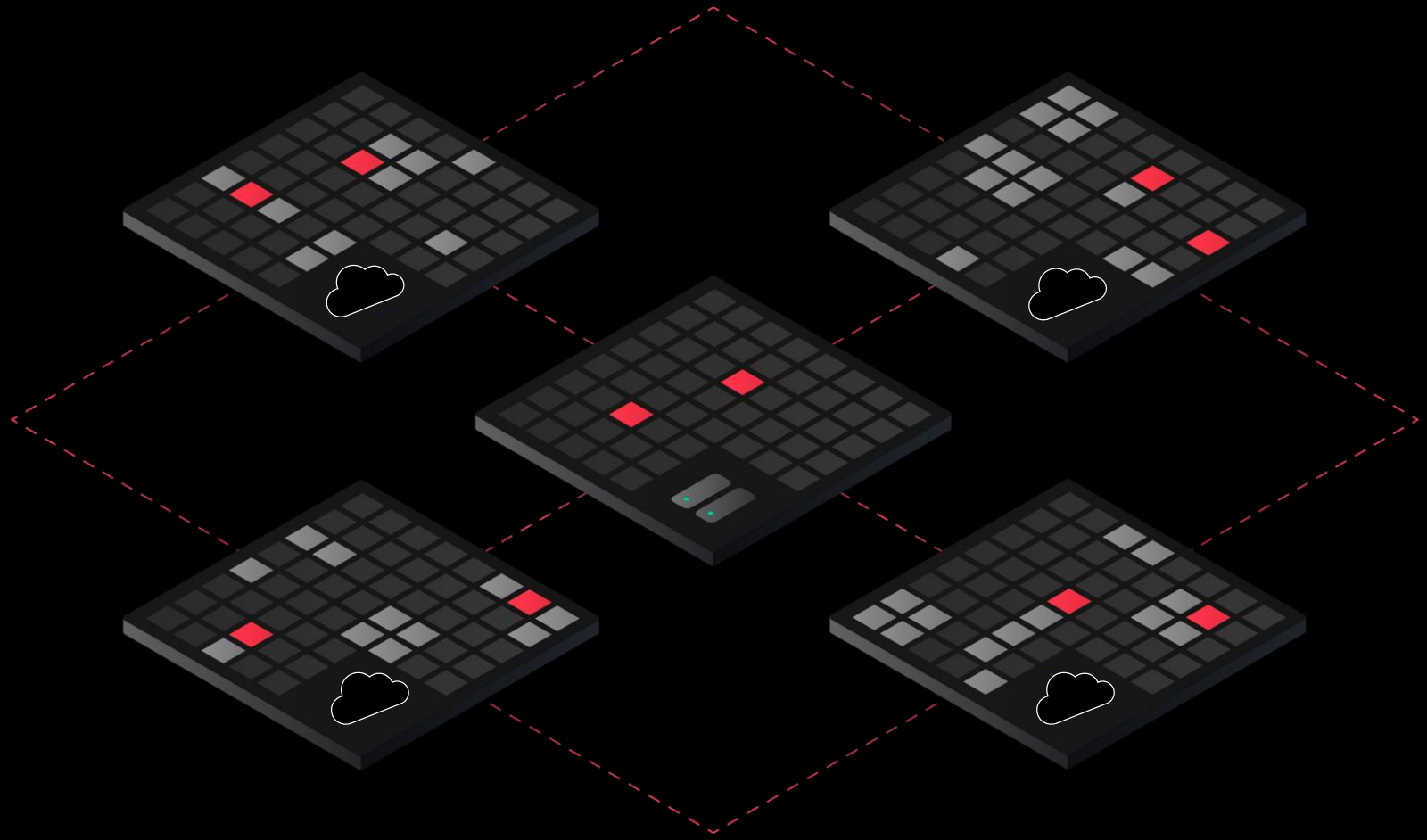


- Trusted perimeter
- Trusted access
- Secured data

But what happens when your applications and infrastructure extend to multiple data centers, the cloud, or all the above?

Securing Modern Infrastructure Can Be Hard.

- No trusted perimeter
- No trusted access
- Unsecured data



The Transition to Cloud and Multi-Cloud

Traditional Data Center
"Static"



Virtual

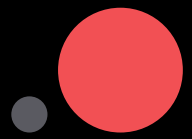
Modern Data Center
"Dynamic"



Private Cloud
Systems of Record

Public Cloud
Systems of Engagement

Security Events by the Numbers



380%

increase over the last 2 years of data theft events



82%

of security events involved a human element



9/10

of web application issues consisted of stolen credentials

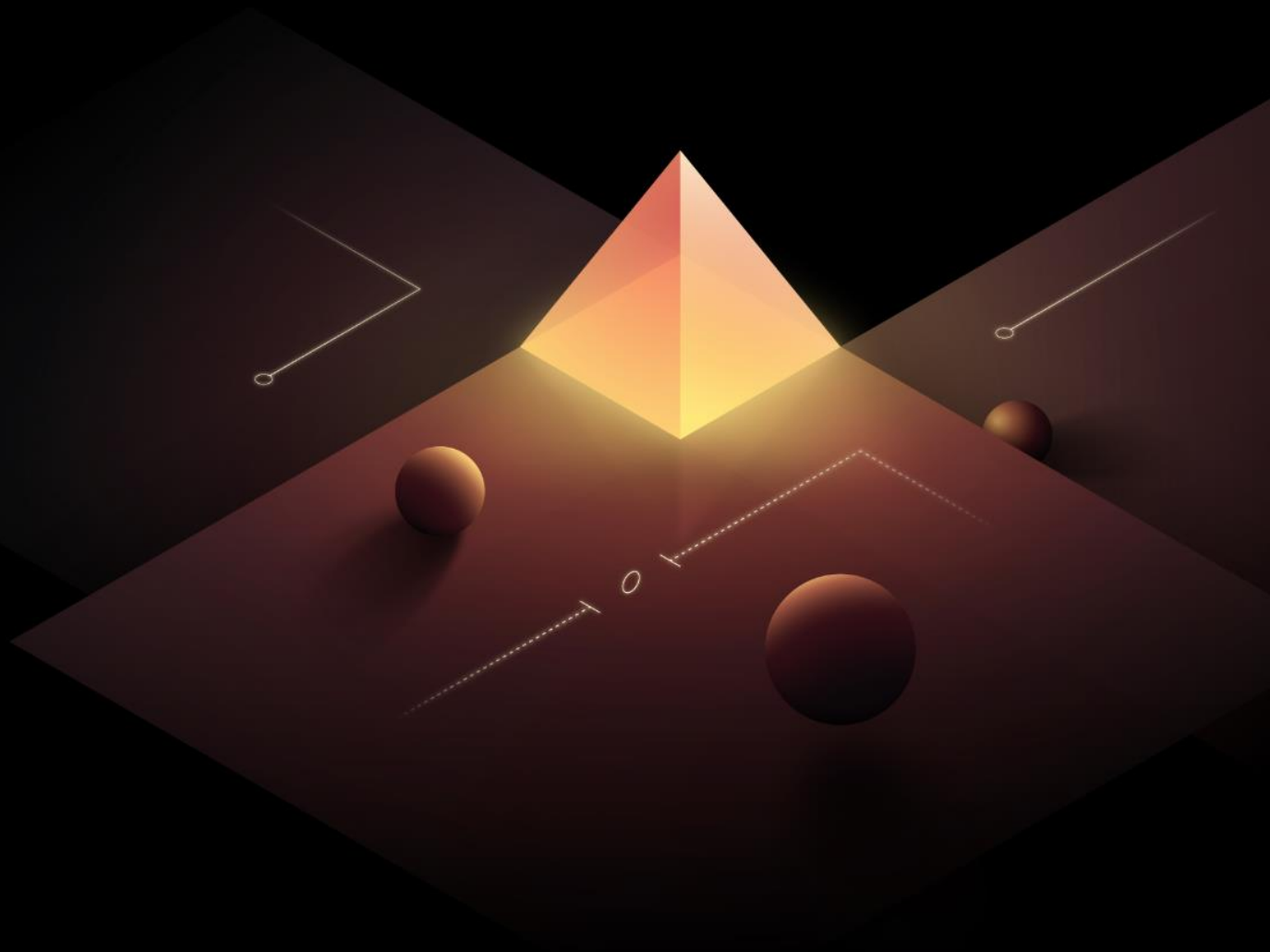


62%

of system intrusions involved a supply chain

Zero Trust Security

Trust Nothing.
Authenticate and
Authorize Everything.

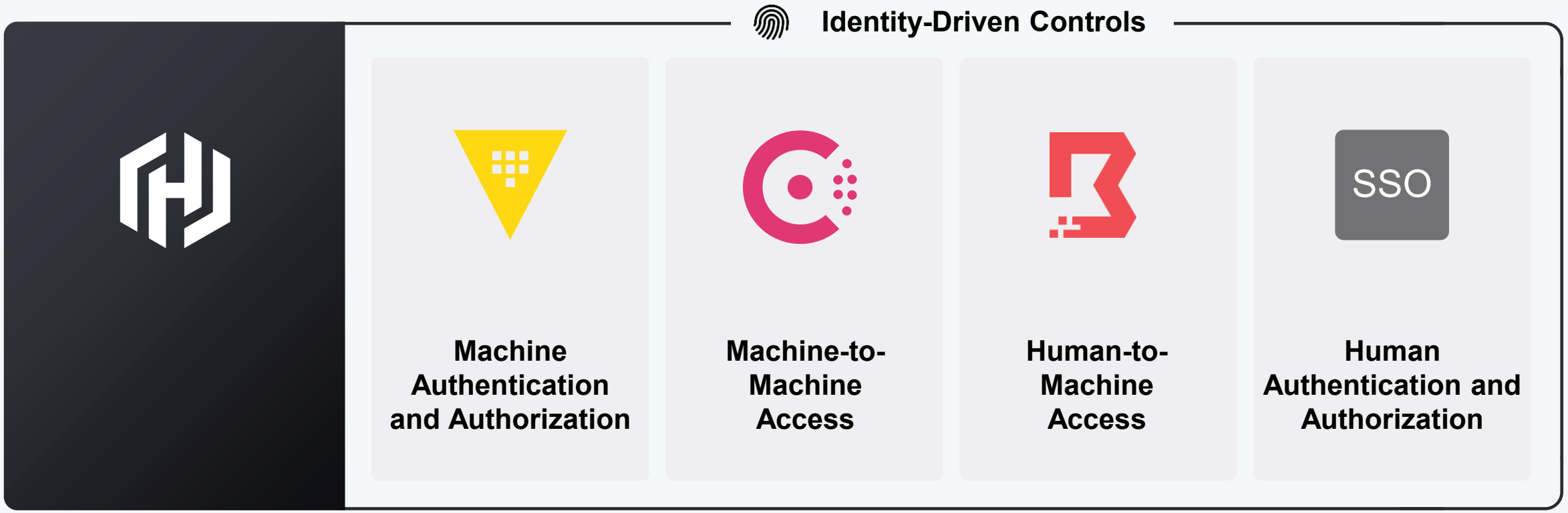


Zero Trust Security

A City of Doors



HashiCorp Multi-Cloud Security

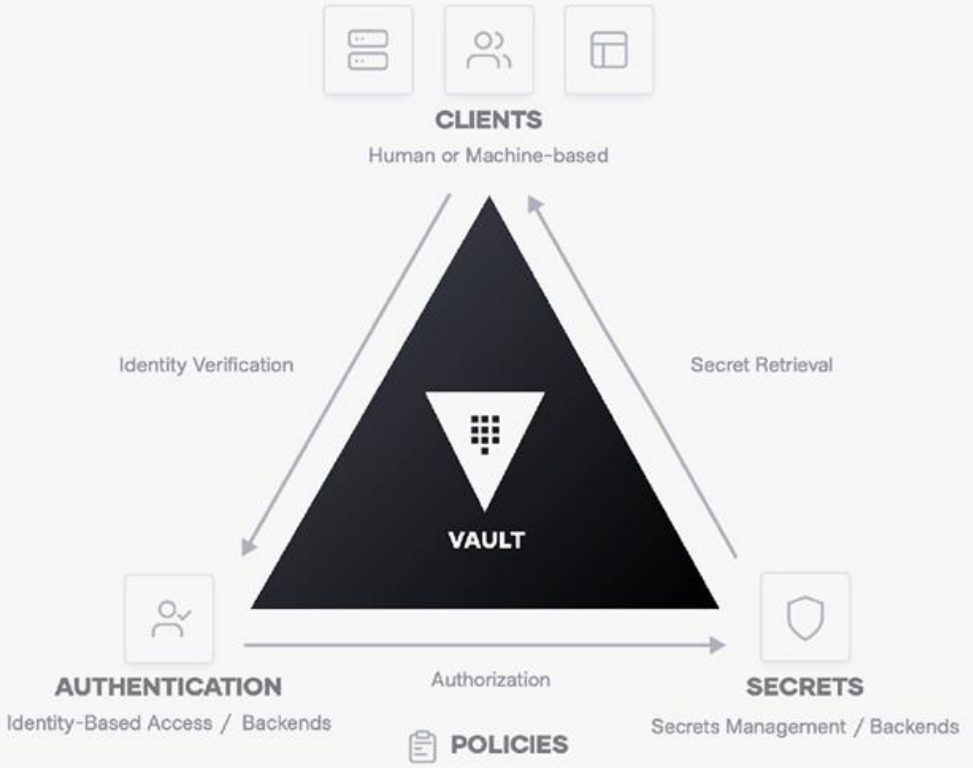


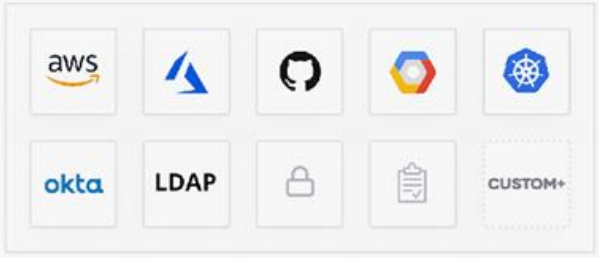


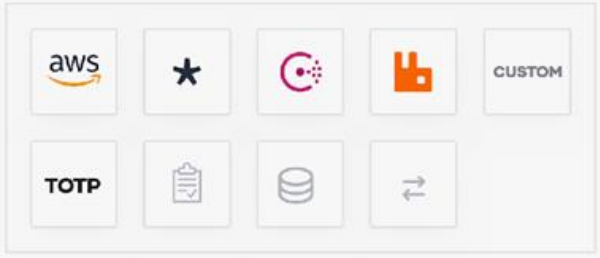
2015

To enable developers and companies to securely store and tightly control access to tokens, passwords, certificates, and encryption keys for protecting machines and applications.

The Vault Approach







600K+

Vault + Kubernetes downloads a year

15.7M+

Vault open-source downloads a year

Trillions

secrets served each year

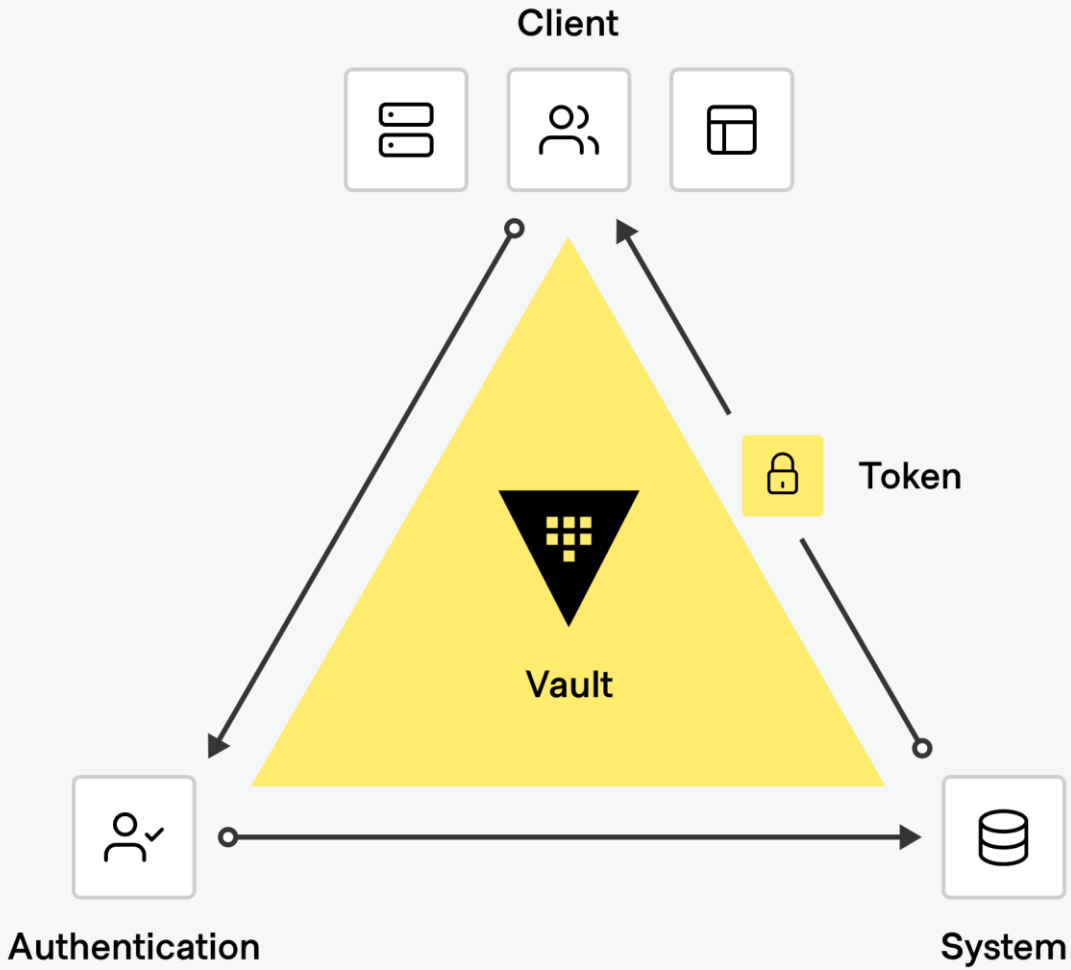
70%

of the top 20 US banks use Vault

Vault

Provides the foundation for cloud security that leverages trusted sources of identity to keep secrets and application data secure in the cloud operating model

- Secrets management to centrally store and protect secrets across clouds and applications
- Data encryption to keep application data secure across environments and workloads
- Advanced data protection to secure workloads and data across traditional systems, clouds, and infrastructure



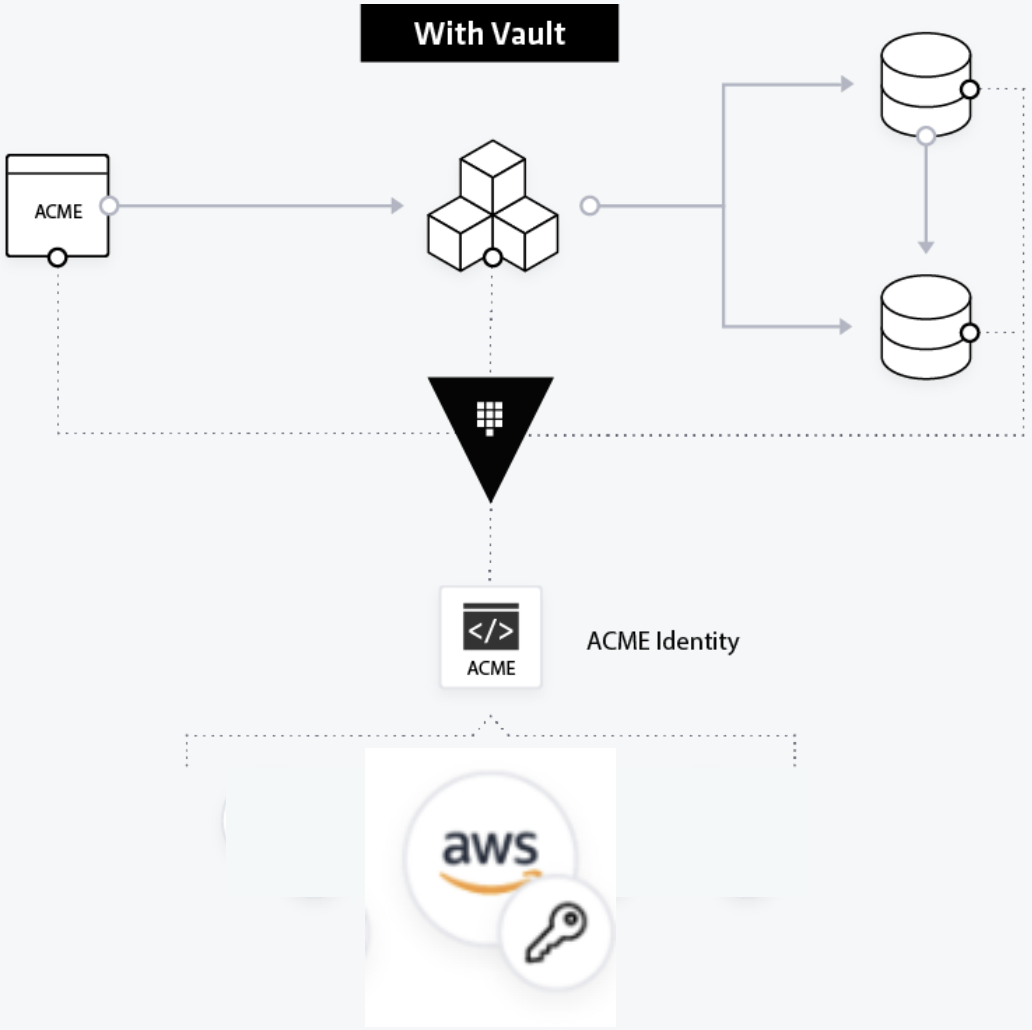
2T+
transactions

1M+
monthly D/Ls

475+
enterprise customers

Guiding Principle
Identity Brokering

- Authenticate and access different clouds, systems, and endpoints using trusted identities
- Leverage multiple identities across different platforms with single policy enforcement
- Integrate trusted identities in the same application workflow to reduce operational overhead



HCP Vault

Available on AWS

hashi.co/cloud-platform



The HashiCorp Cloud Platform Vision



Push-button deployment

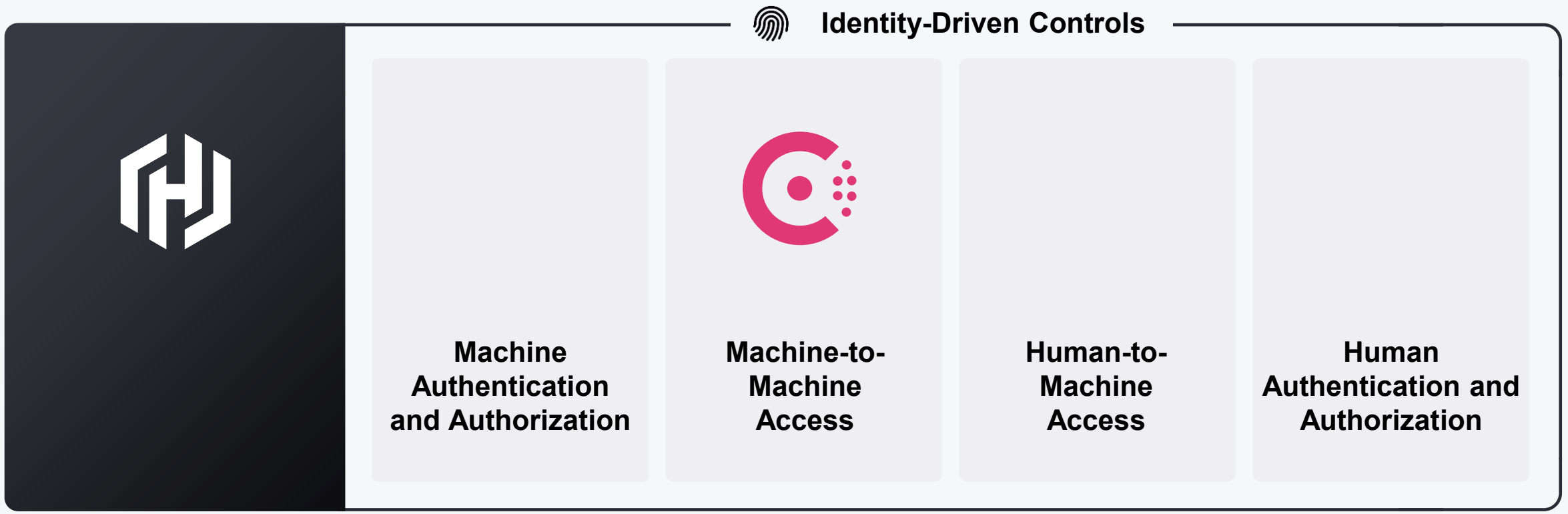


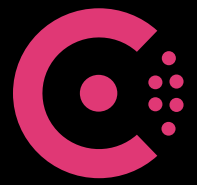
Fully managed infrastructure



One multi-cloud workflow

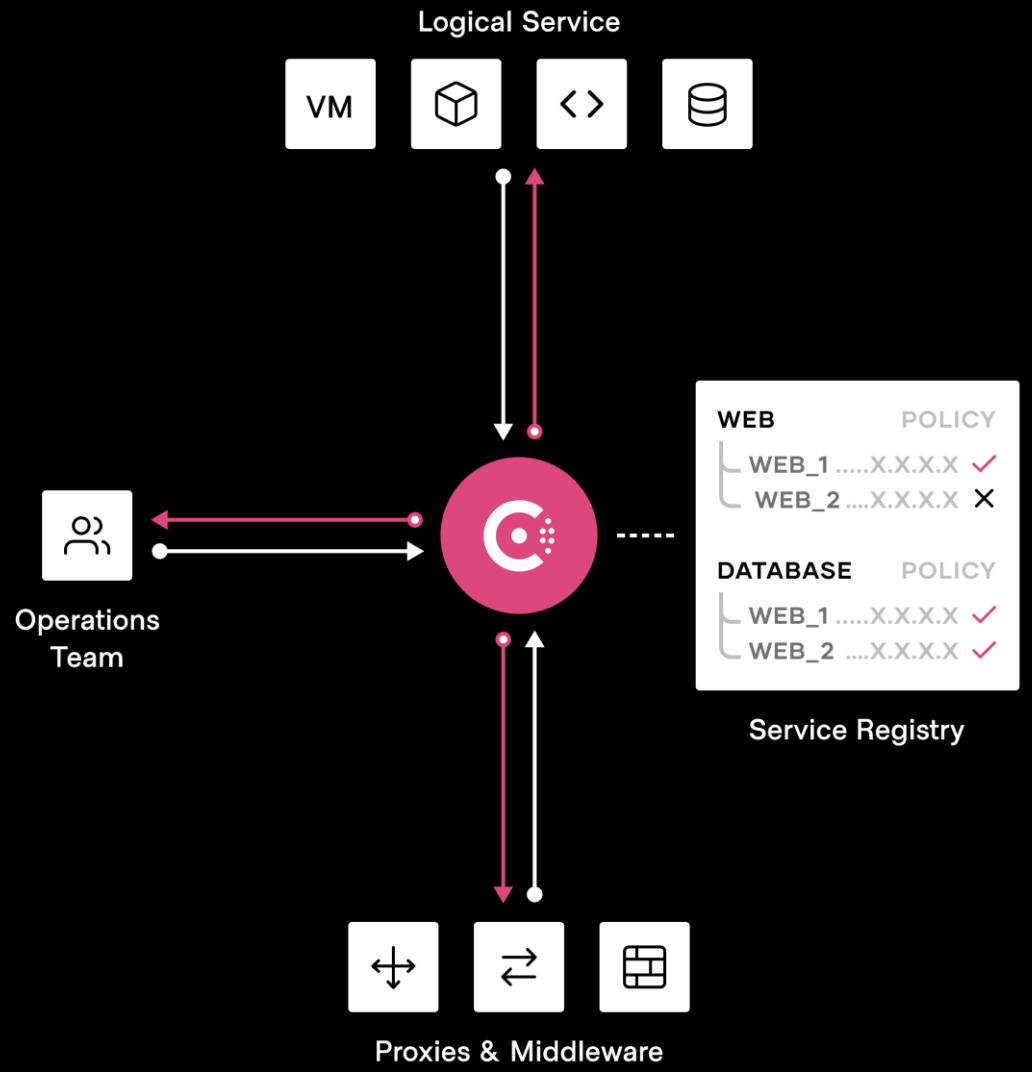
HashiCorp Multi-Cloud Security



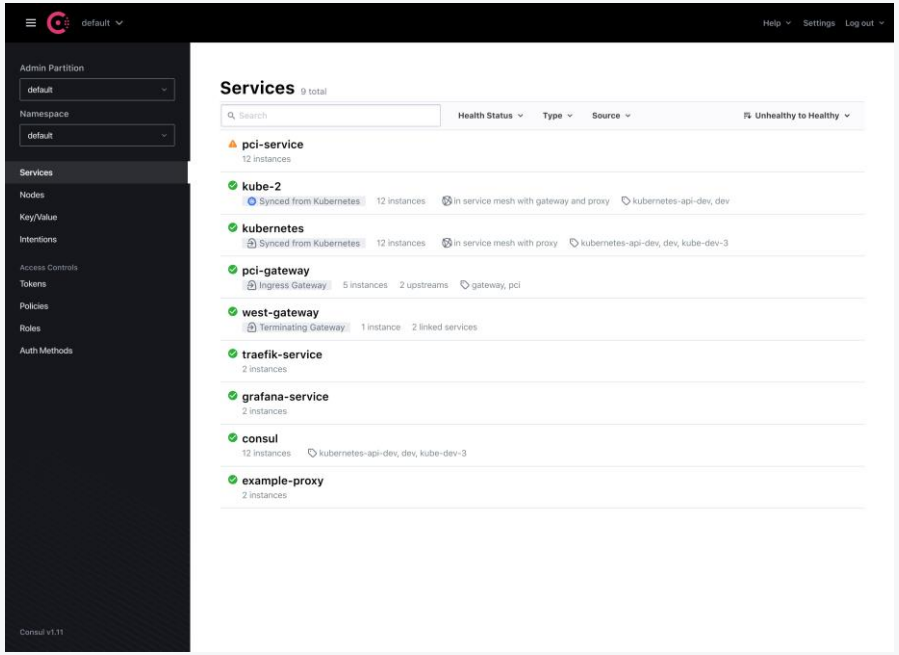


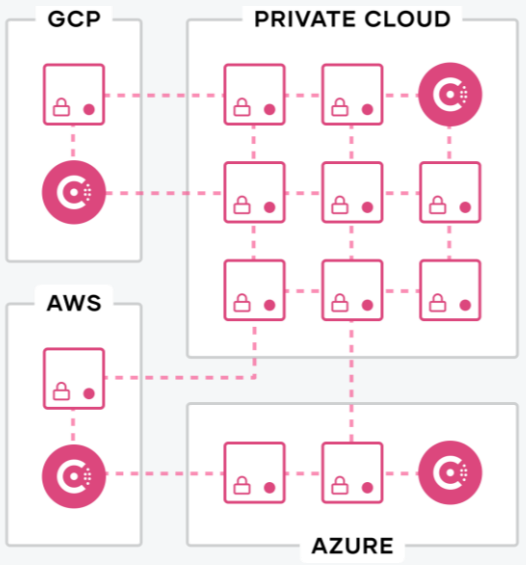
Service Networking Across Any Cloud

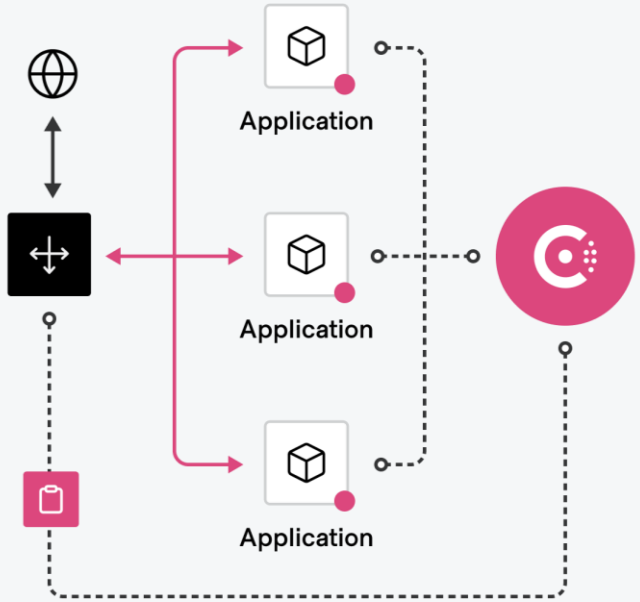
Automate network configurations, discover services, and enable secure connectivity across any cloud or runtime.



What is Consul

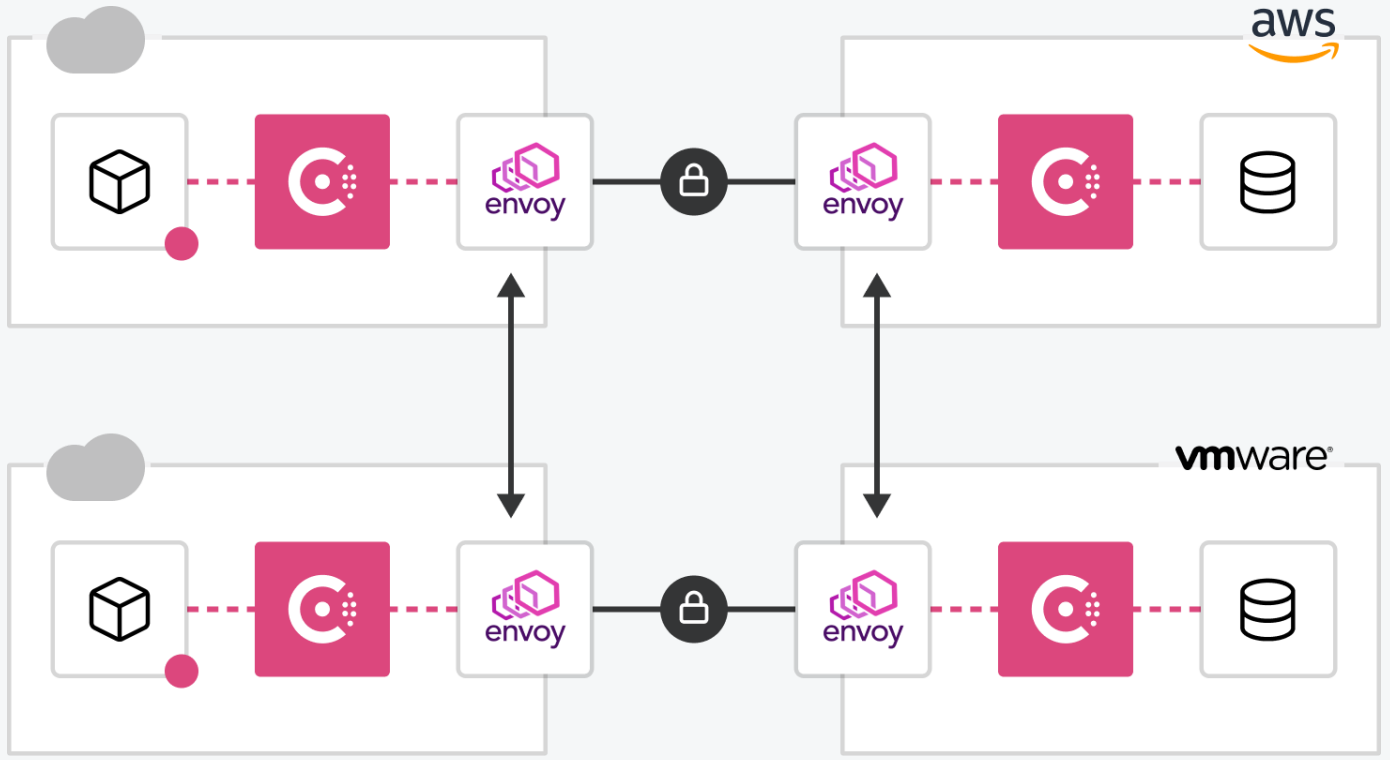






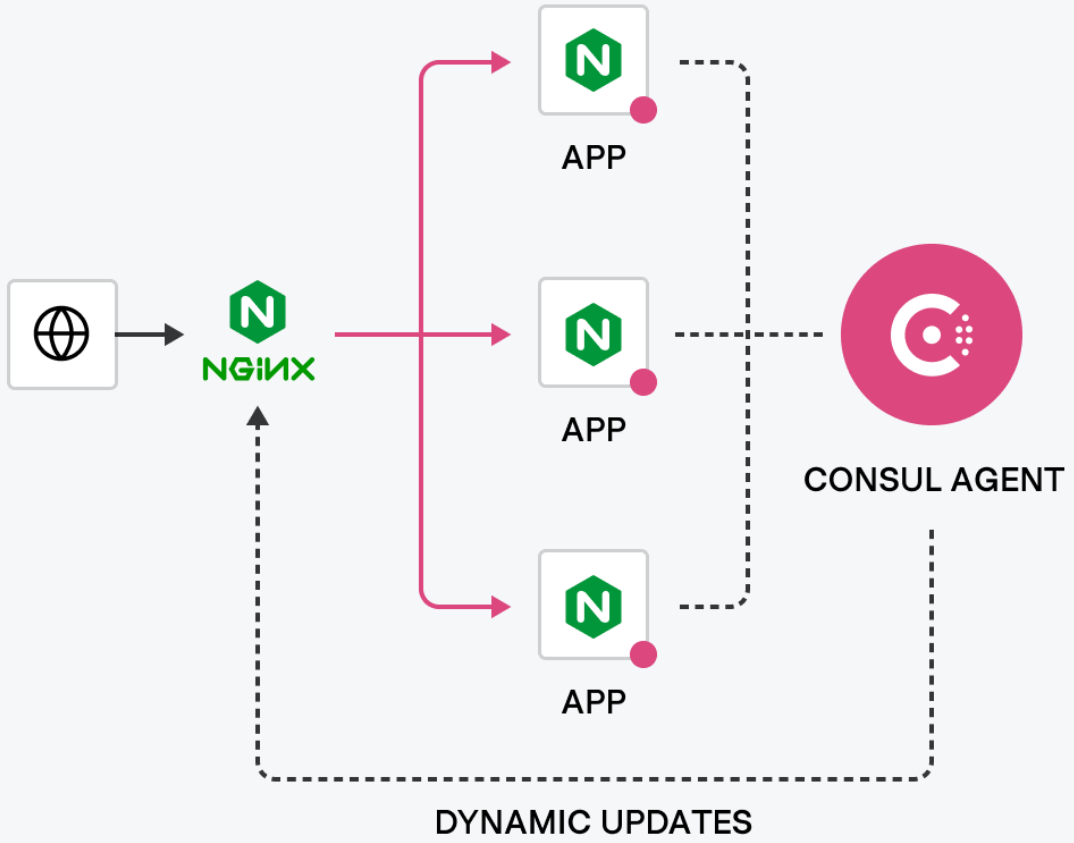
Multi-Cloud Service Mesh

Secure service-to-service connection, authorization, and encryption



Network Infrastructure Automation

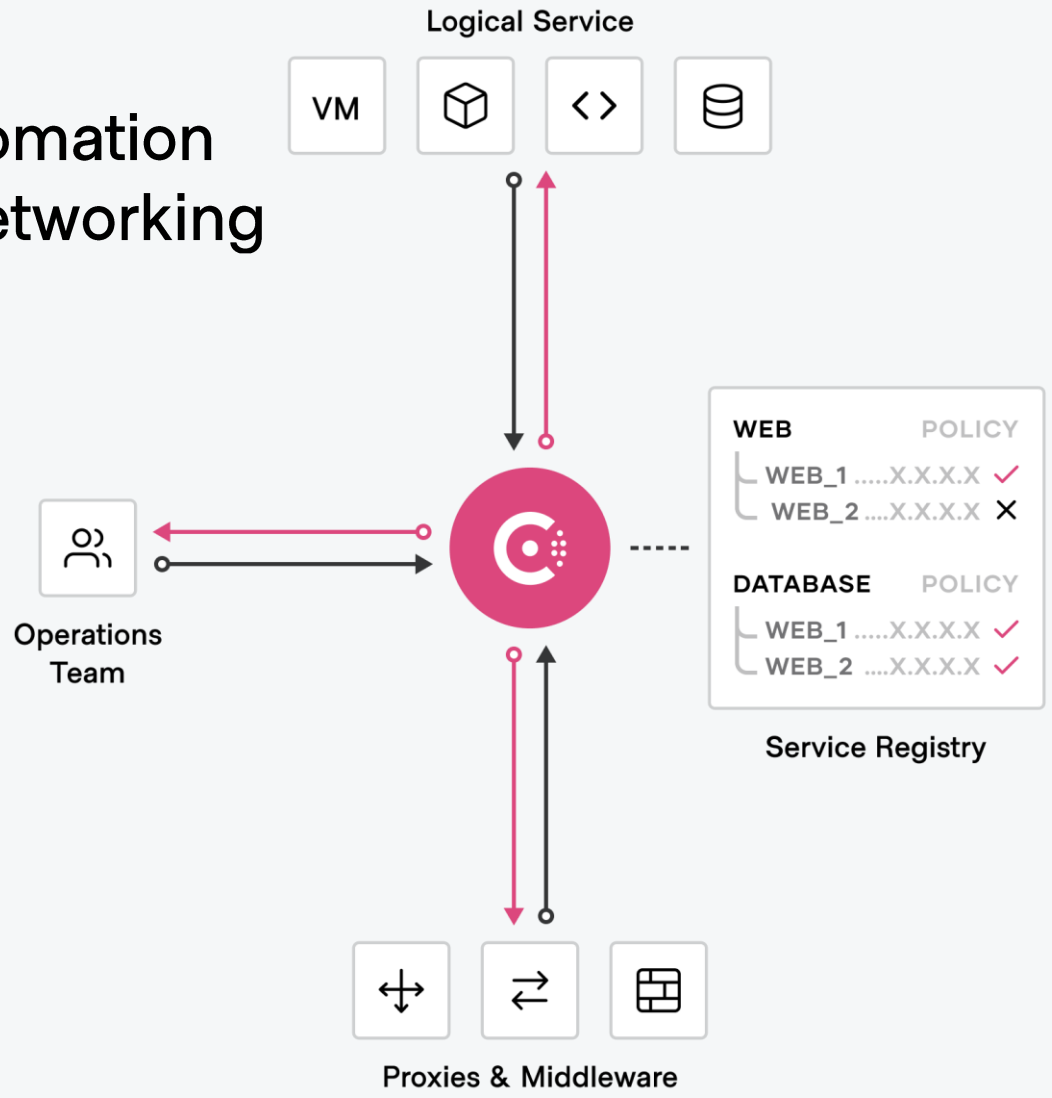
Easily deploy, manage, and optimize network infrastructure



Consul

Provides a foundation of cloud network automation using a shared registry for service-based networking

- Allows networking operations to decouple from IP addresses to support dynamic networking
- Provides automated services networking and security based on logical services
- Services can be discovered, connected, and secured with service name as identity
- Captures telemetry data which can be observed via UI or exported to third-party tools

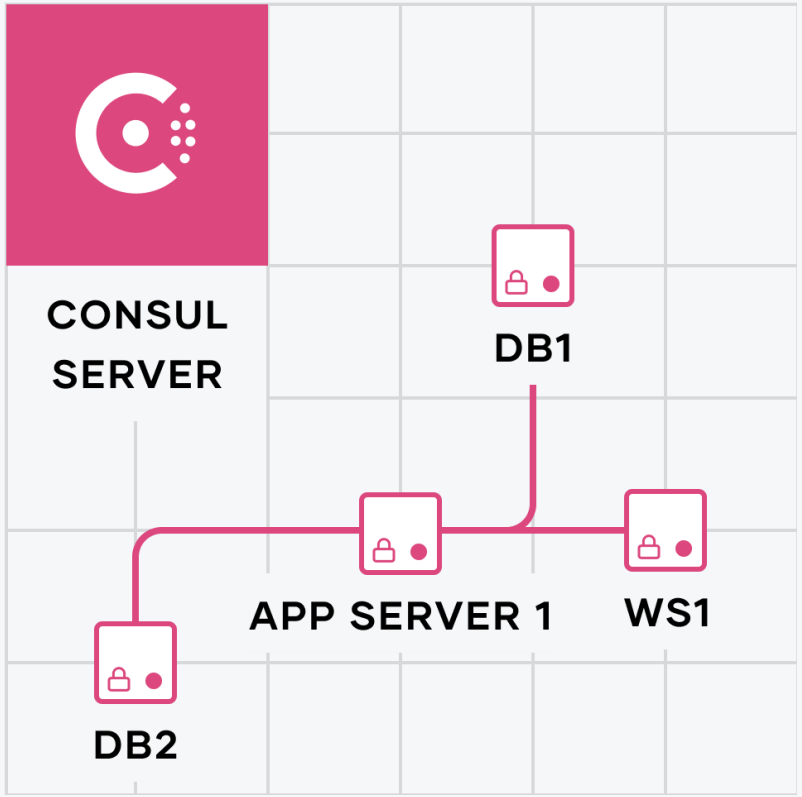


2T+
transactions

50K+
used at scale with 50K+ agents

Guiding Principle **Application-Based Networking**

- Allow networking operations to decouple from IP addresses
- Automated networking and security based on logical services
- Services can be discovered, connected, and secured with service name as identity
- Enable secure networking to happen at the application layer and align it with CI/CD



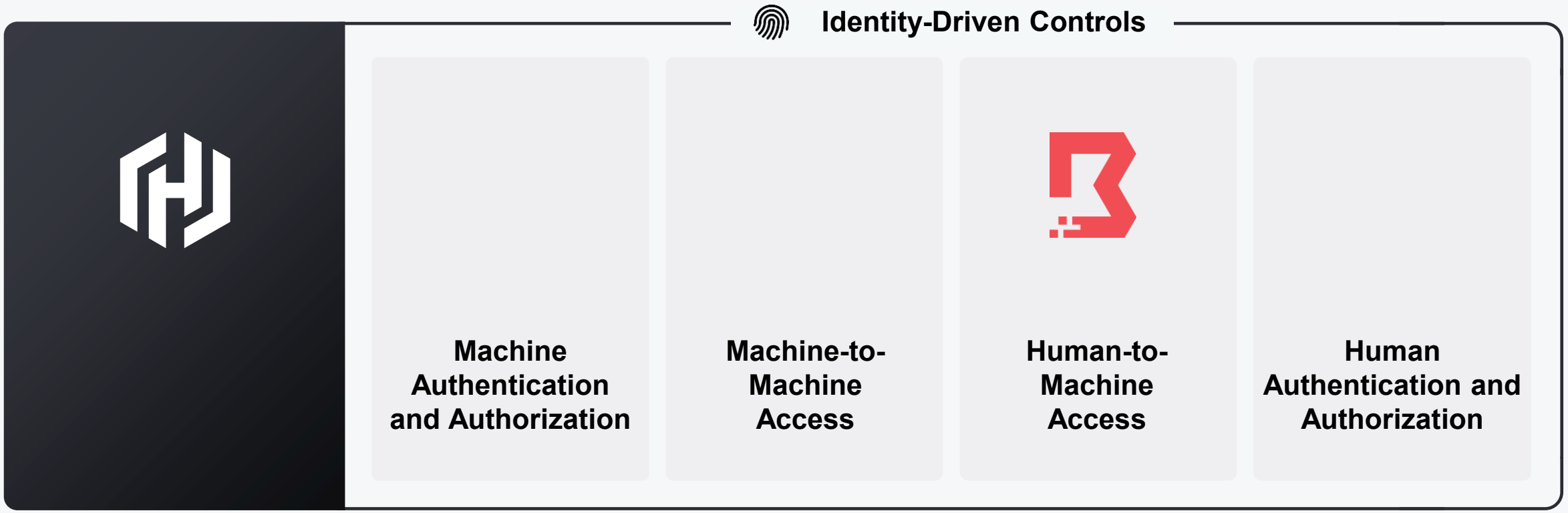
HCP Consul

Available on AWS

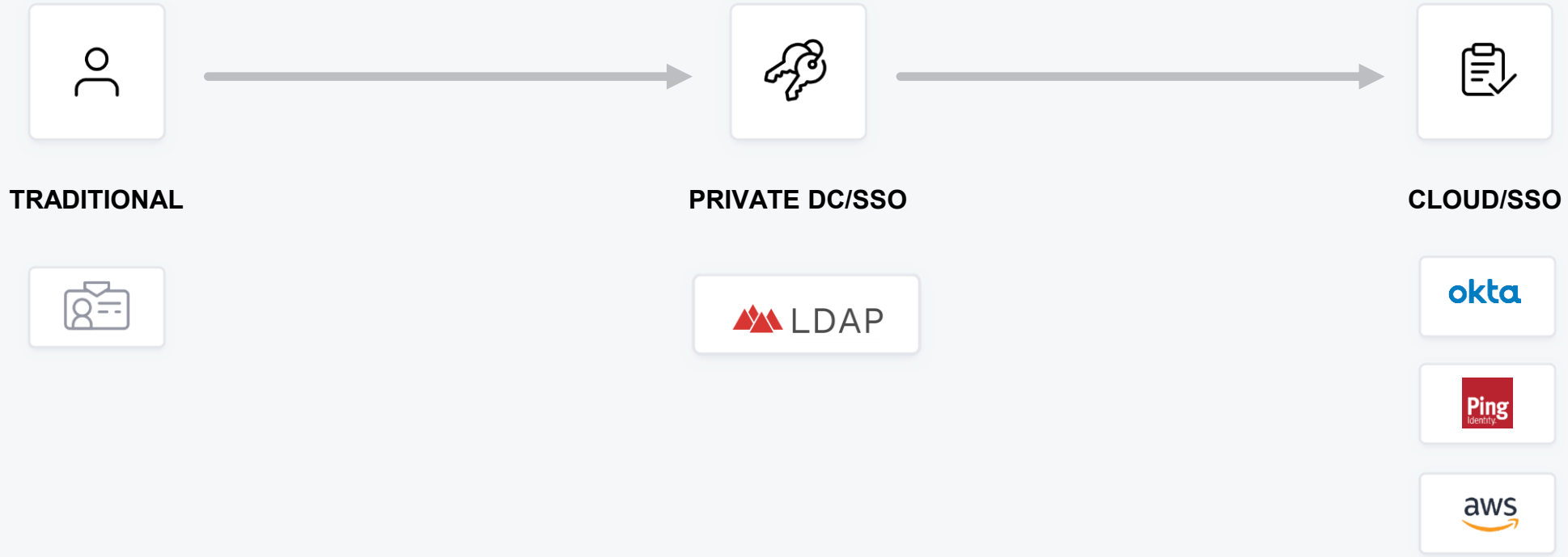
hashi.co/cloud-platform



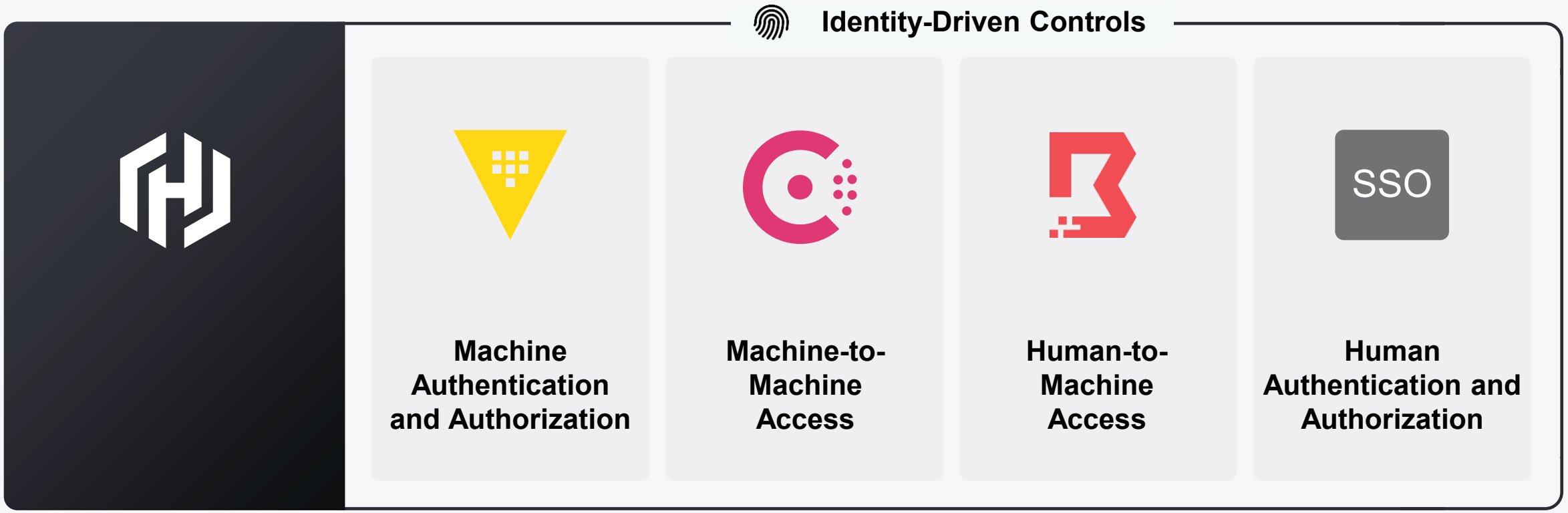
HashiCorp Multi-Cloud Security



Establishing user identity



HashiCorp Multi-Cloud Security



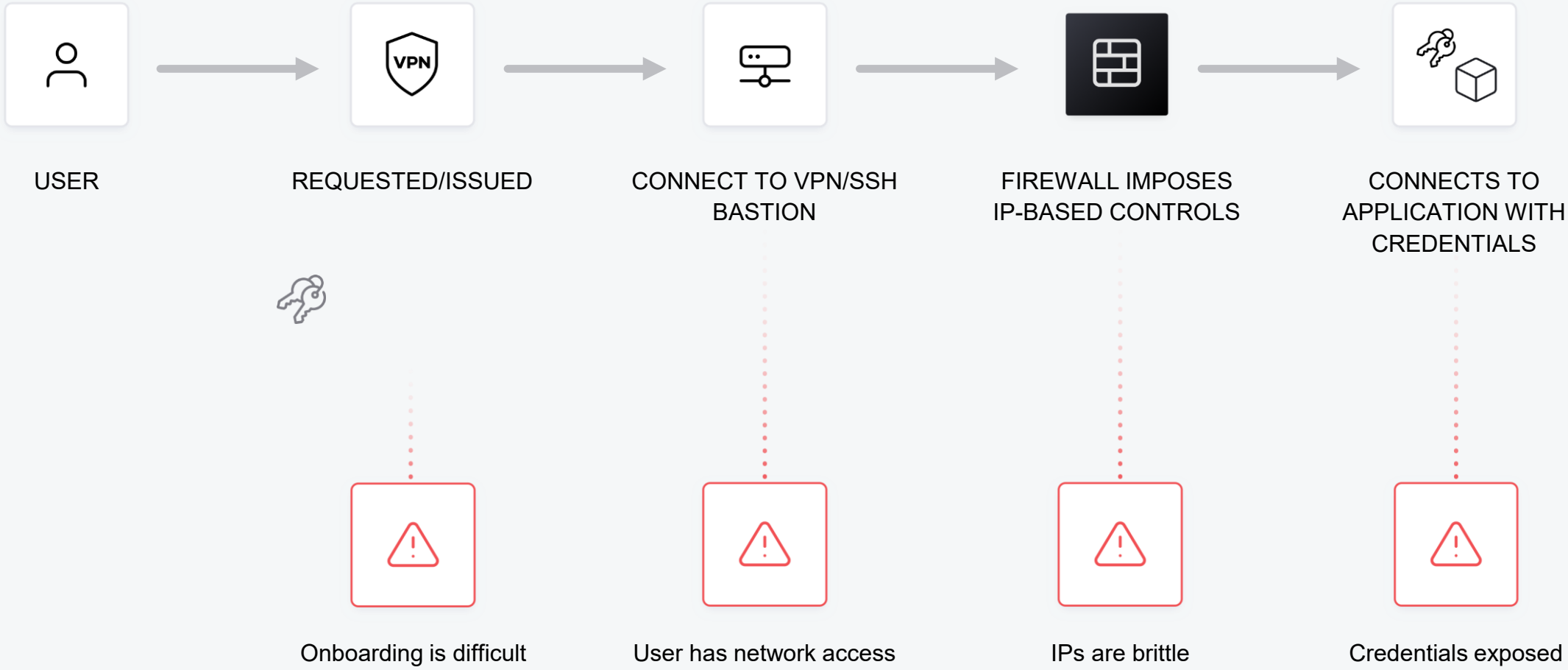
HCP Boundary

Available on AWS

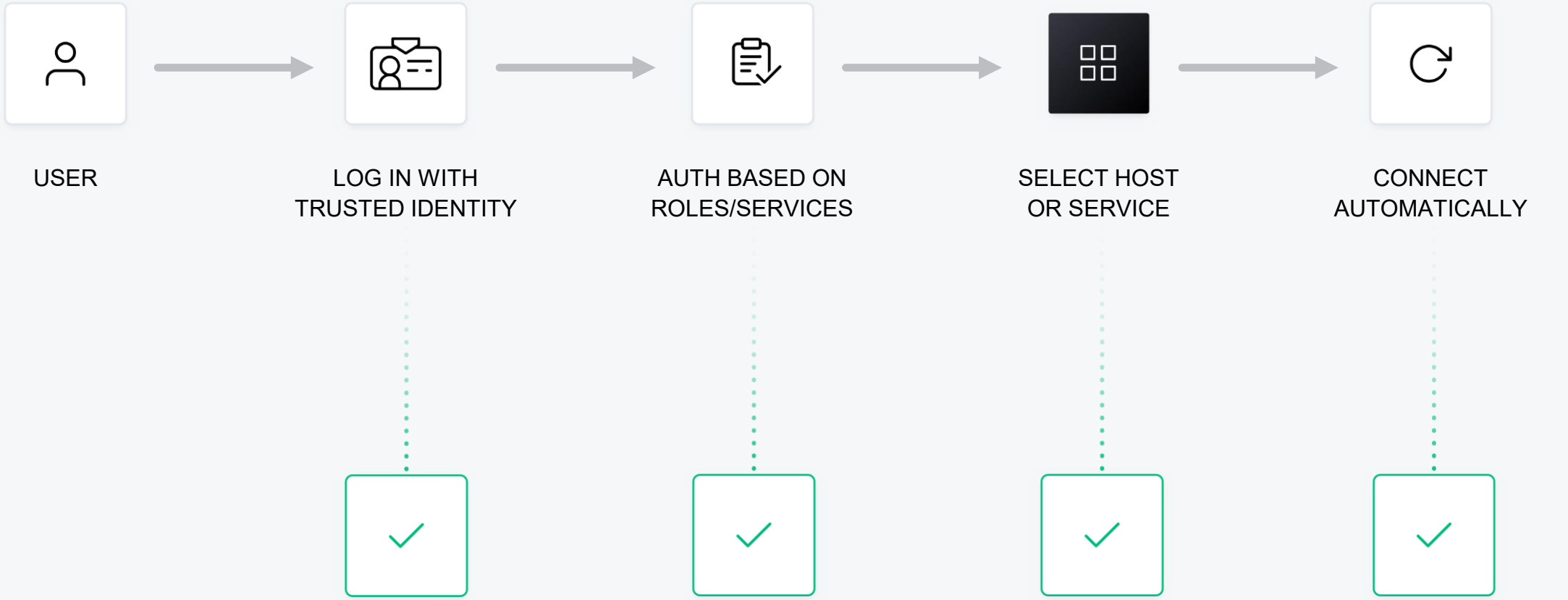
hashi.co/cloud-platform



Traditional workflow for access

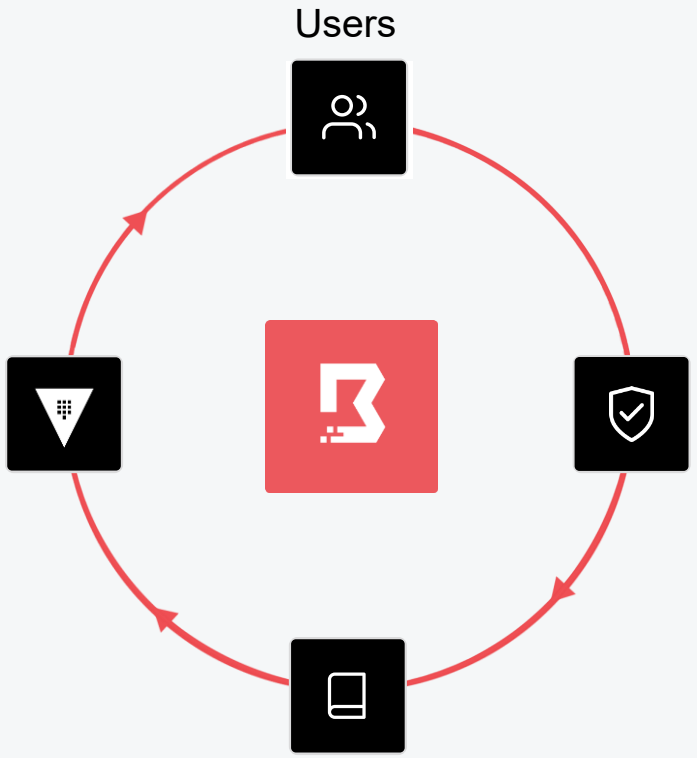


Dynamic workflow for access



HashiCorp Boundary

Simple and secure remote access
Access any system from anywhere based on user identity.



Access

Access any remote system, host, or services with dynamic secrets and just-in-time credentials.

Custom +

Authenticate and Authorize

Authenticate with any trusted identity provider and enable fine-grained role-based authorization

Custom +

Connect

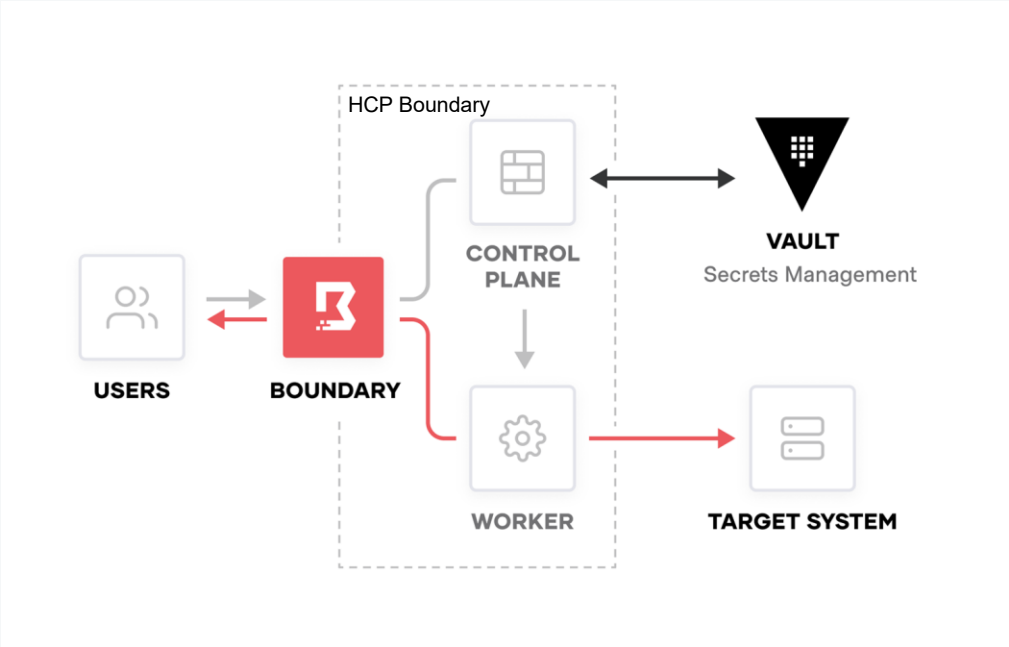
Dynamically connect any service registry so that hosts and service catalogs are up to date

Custom +

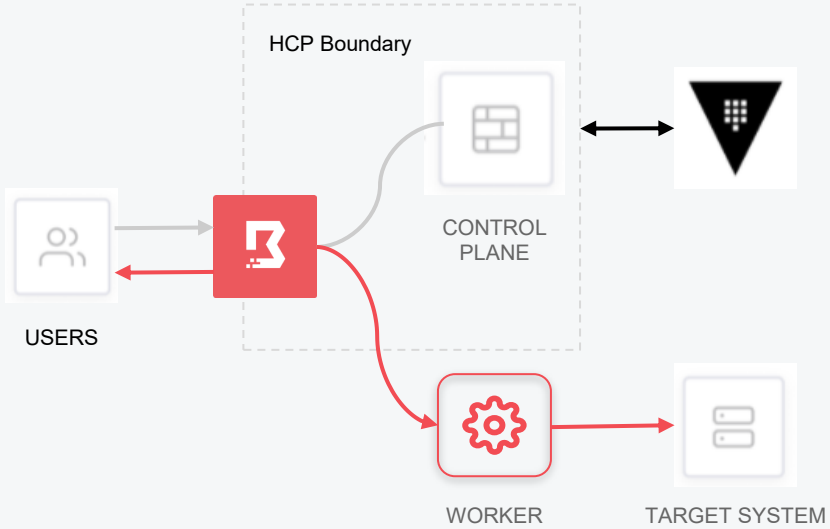
HCP Boundary access model

Boundary provides a secure way to access critical systems
without having to manage credentials or expose the network

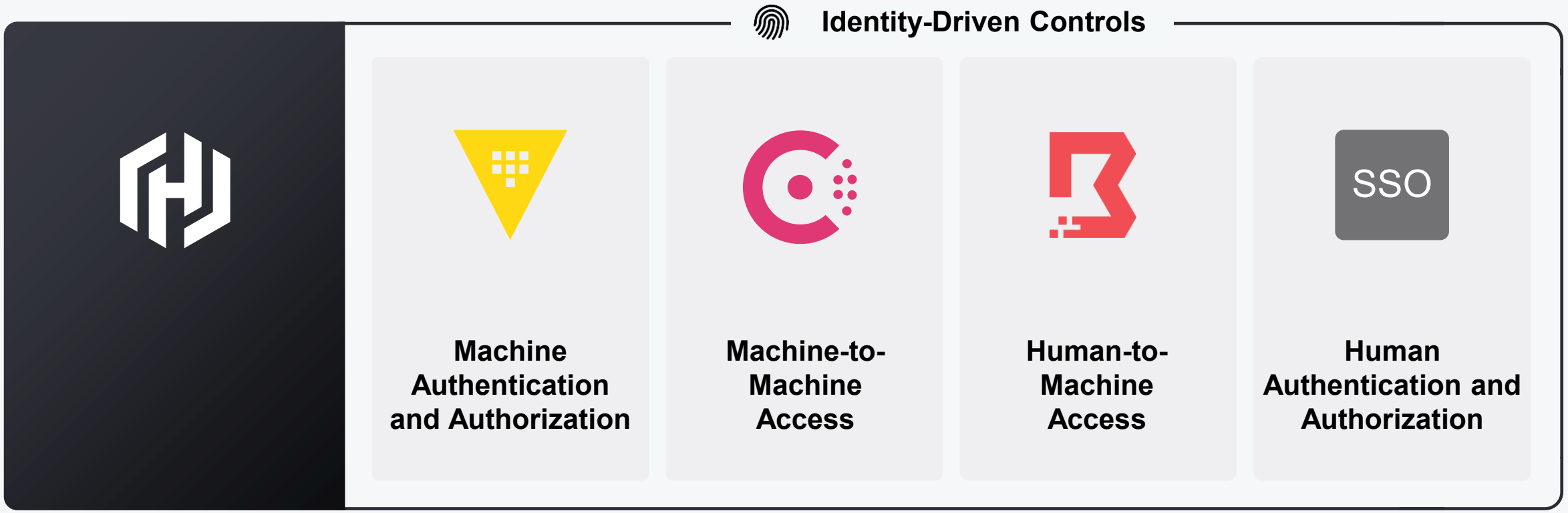
Fully-managed HCP Boundary deployment



HCP Boundary with self-managed workers

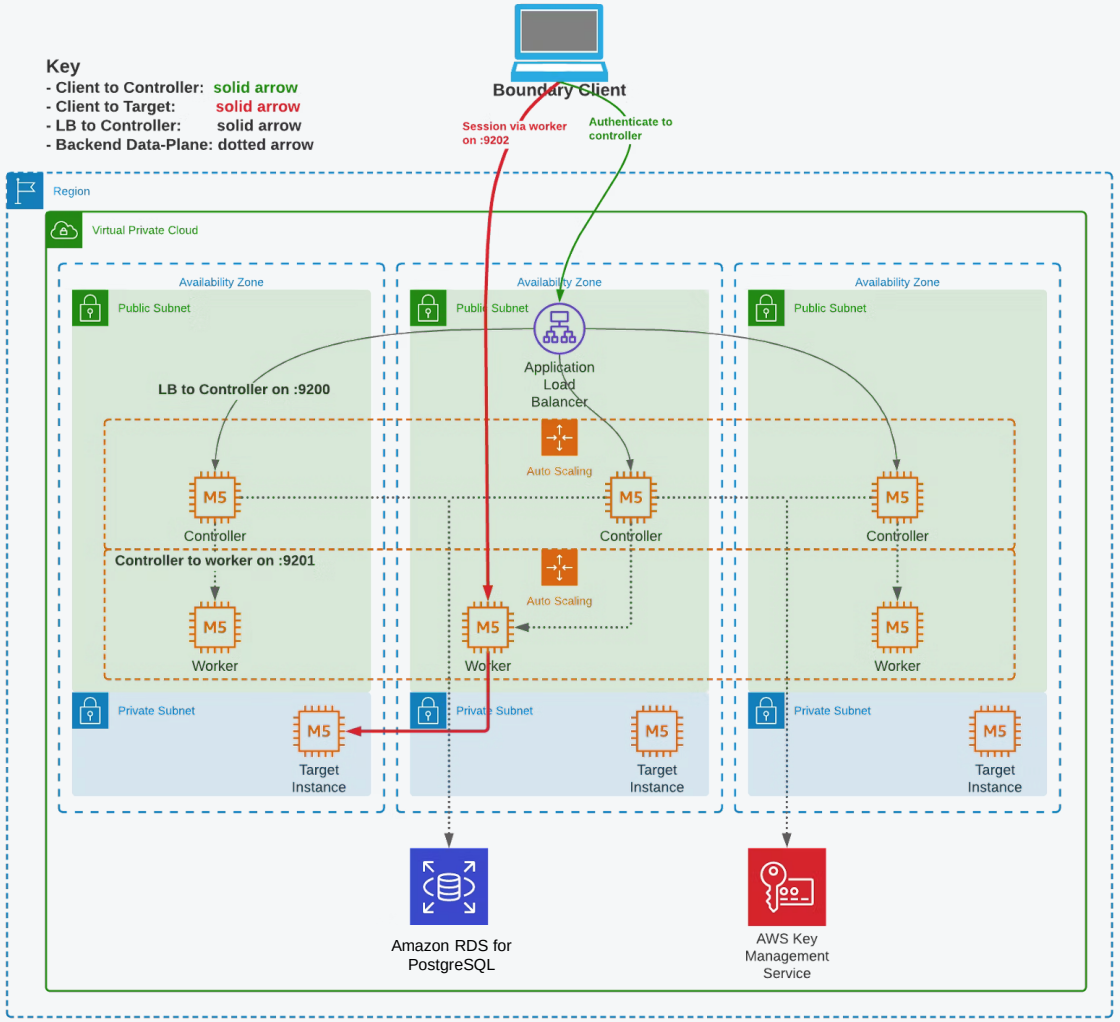


HashiCorp Multi-Cloud Security



Zero Trust Infrastructure on AWS

- **Vault – Machine Authentication:** Leverage AWS Identity and Access Management (IAM) Auth to service AWS native workflows and generate credentials with AWS secrets engine.
- **Consul Machine to Machine Access**: Using Consul's service registry, route access to Amazon EC2–based applications.
- **Boundary – Human Authentication:** Leverage AWS KMS to encrypt host catalogs, establish sessions to Amazon EC2–based hosts via dynamic host catalogs.
- **Full Integration with HCP:** All ZTS services interfaceable over HCP to AWS via HVN.



Thank you!



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.