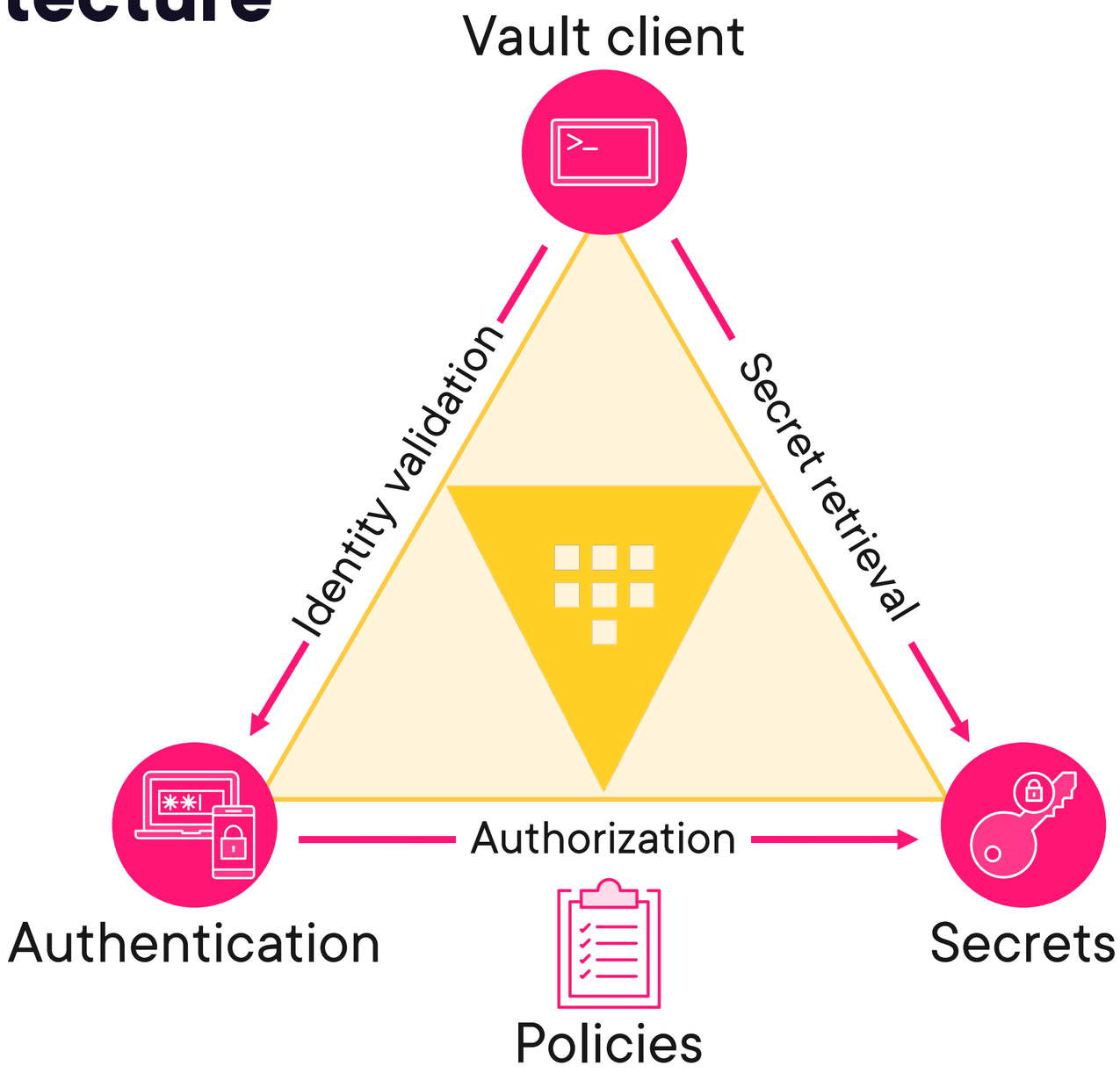
Authentication Methods for Vault Associate (003)

Authentication Method Basics

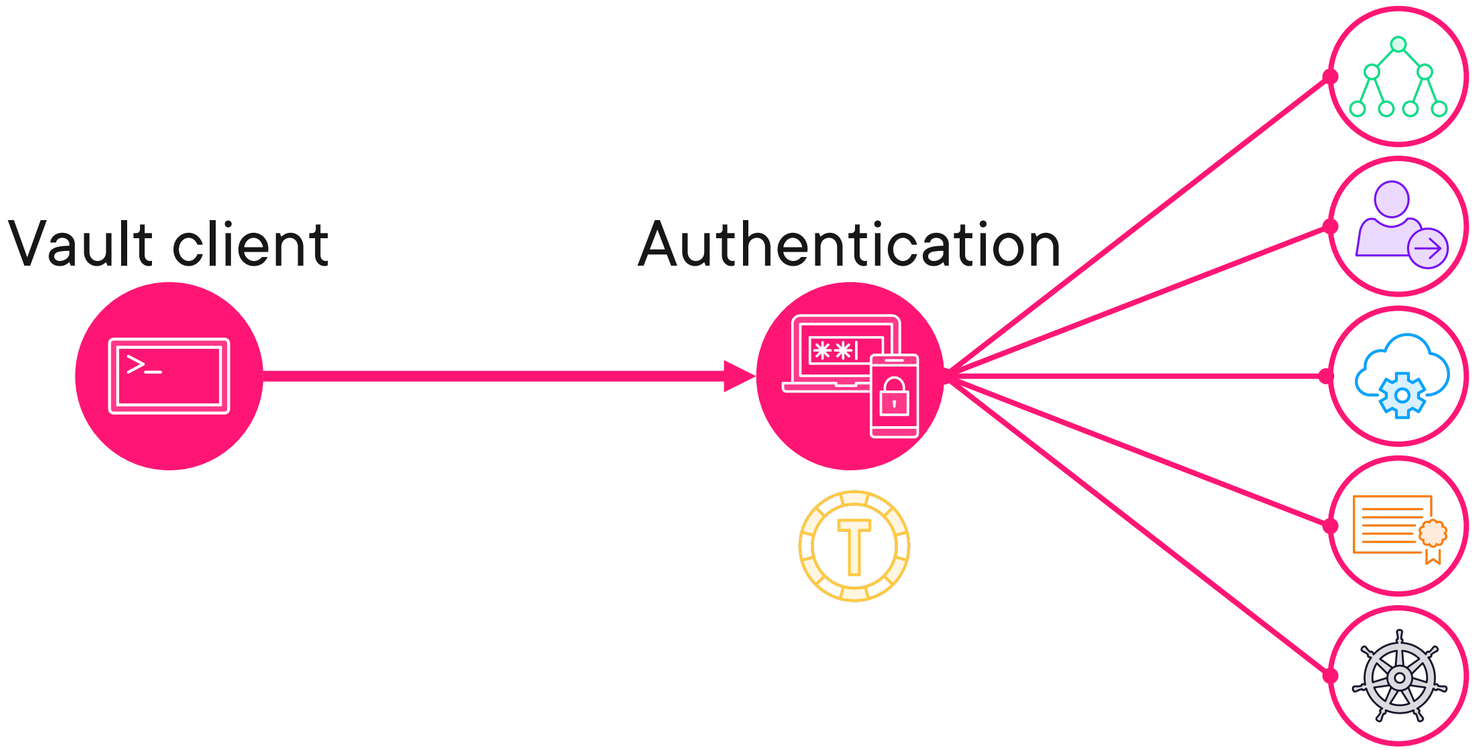
Ned Bellavance
HashiCorp Certified Instructor

@nedinthecloud | nedinthecloud.com

Vault Architecture



Vault Authentication



Authentication Methods

Plugin-based architecture

- Built-in, third-party, and custom

Enabling auth methods

- /sys/auth
- Multiples instances supported
- Enabled by CLI, API, or UI
- Defaults to auth method name

Token method

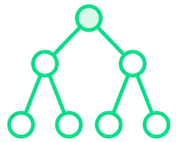
- Enabled by default
- Cannot be moved or disabled
- One instance only

Authentication Method Categories

Vault native: Token, Userpass, AppRole

Cloud provider: AWS, Azure, Google Cloud, Okta

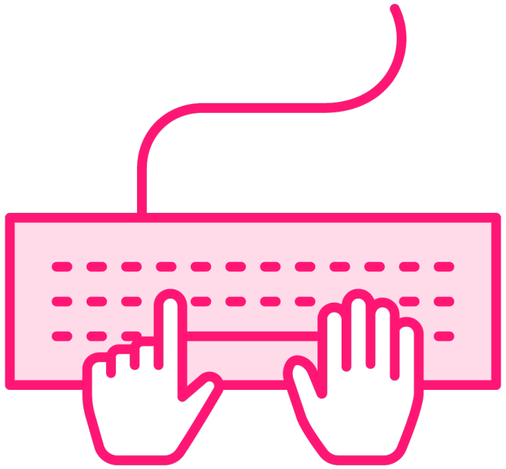
Cloud native: Kubernetes, SAML, OIDC, JWT



Traditional: LDAP, RADIUS, Kerberos, TLS certificates

Choosing an Auth Method

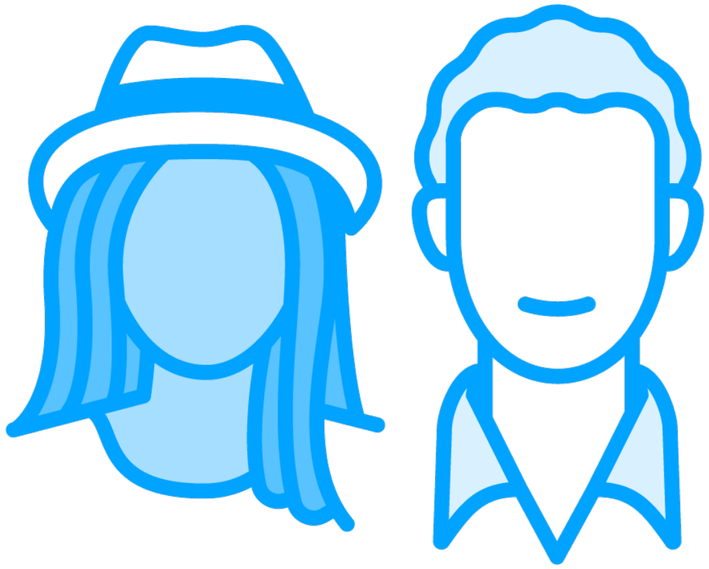
Who is going to access Vault?



How are they going to access it?

What do they use today?

Explain the difference between human & system authentication methods



Interactive

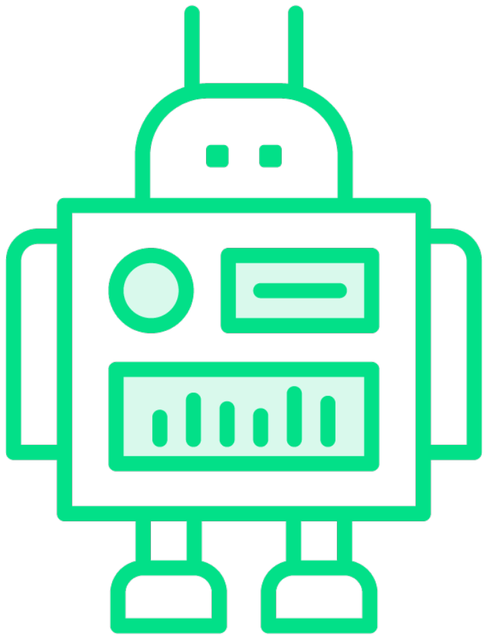
Relatively slow

Personal knowledge

MFA okay

Examples

- Userpass, LDAP, GitHub



Non-interactive

Relatively fast

Machine identity or properties

Examples

- TLS certificates, AWS, AppRole

Enabling an Auth Method

Collect information about the provider

All methods enabled on /sys/auth

Methods enabled on a path

- Defaults to method name
- Moving revokes leases

Tuning settings are common to all methods

Configuration settings are method specific

- Consult documentation