HashiCorp | VENAFI®

Protecting Machine Identities: Blueprint for the Cloud Operating Model

Accelerate DevOps Securely with HashiCorp and Venafi

Executive Summary

Digital transformation requires businesses to be more agile with technology. Today's technology needs to:

- Run anywhere
- Change fast
- Automate everything

This means speed rules! At the heart of this fundamental change is the HashiCorp Cloud Operating Model, where freedom of what, where and how you run is now under the control of developers. To run fast developers need the easiest and fastest building blocks. In this model, security teams have the opportunity to provide common services to accelerate development and keep the business safe.

Identity is the new perimeter and a required element in every multi-cloud strategy. Cloud services, containers, service meshes and container orchestration platforms like Kubernetes all rely on machine identities such as X.509 TLS certificates for secure machine-to-machine communication. Understanding what is good or bad, private or public, allowed or not depends on machine identities.

Venafi and HashiCorp provide the proven blueprint for Machine Identity Protection, providing security teams with smart policy enforcement of machine identities and DevOps teams the speed and agility they require. Venafi works together with HashiCorp Terraform, Vault, and Consul to deliver on the business need for speed as part of today and tomorrow's cloud strategy.

The Rules of Digital Transformation

Consistency, Agility, Speed

It's an exciting time to drive new business growth and innovation. Cloud, mobile, AI, big data, and IoT technologies create entirely new ways for businesses to engage customers and deliver value. To accomplish these audacious business goals, DevOps teams must:

- Run anywhere: Build environment-agnostic applications that can be deployed anywhere quickly.
- Change fast: Make updates constantly without ever stopping service and fail fast.
- Automate everything: Automate the software life cycle using their favorite tools to deliver new apps and features faster, and eliminate errors like costly outages.

CIO Strategy

To accomplish these business and technical goals, CIOs are charting a course for a multi-cloud strategy. According to Forrester Research, 74 percent[1] of North American and European enterprise infrastructure decision makers define their strategy as hybrid. This drives competition and freedom to choose.

As organizations undergo digital transformation, core business applications often continue to reside on infrastructure in data centers, while greenfield applications run in a mix of public and private cloud environments. Getting locked into any single cloud provider's strategy may be the biggest career limiting decision a CIO can make today.

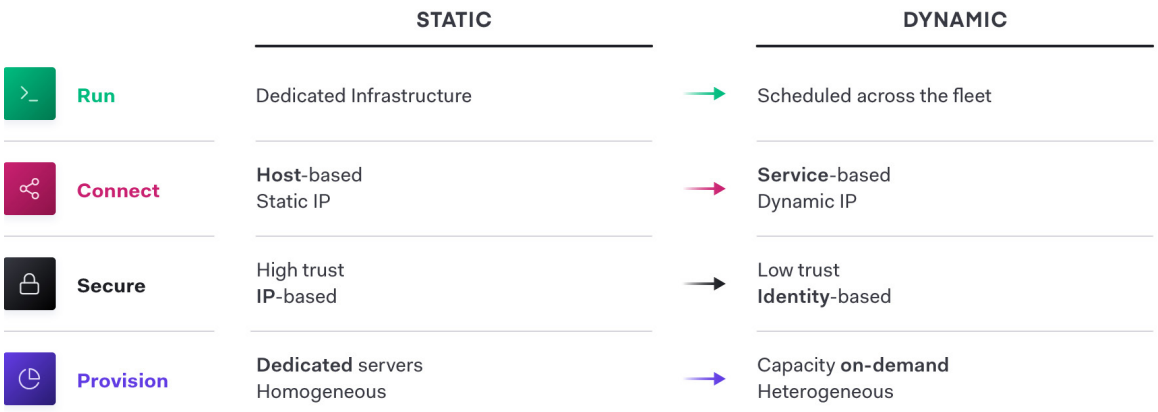
Multi-Cloud: The Norm

An essential implication of this transition to the cloud is the shift from "static" infrastructure to "dynamic" infrastructure—from a focus on configuration and management of a static fleet of IT resources, to provisioning, securing, connecting, and running dynamic resources on demand. In these dynamic environments, identity is the new perimeter and a required element in every multi-cloud strategy.

Every cloud environment is different: APIs, services, applications, security and operations. This is chaos and a risky recipe. For enterprise IT teams, there is an opportunity to move to a cloud operating model that provides consistency, speed, and a simple development platform for application development teams.

To unlock the fastest path to value of the cloud, enterprises must consider how to industrialize the application and security delivery processes across each layer of the cloud and across multiple clouds: embracing the cloud operating model, and tuning people, process, and tools to it to enable speed, agility, consistency. This is the future.

[1] Nelson, Lauren. Forrester. Top 10 Facts Every Tech Leader Should Know About Hybrid Cloud. April 25, 2018.



Provision, Secure, Connect, and Run: The HashiCorp Model for Moving from Static to Dynamic Infrastructure

New Battle Line Drawn: Identity

As business drives to new levels of digital transformation, a slew of adversaries seek to profit from it. In a world without firewalls, self-contained networks or perimeters, the future of securing businesses and customers is identity. Identity defines who and what is trusted, what is private and who and what is not trusted.

Machine identities secure the cyberworld we all live in and X.509 certificates are the most common form of machine identity. They establish trust for web services, segmentation in service mesh, and relationships within clusters. Security must be enforced in real-time, which means that security teams must make it easy for developers to access trusted machine identities.

Identity in the Age of Digital Transformation

The Exploding Number of Machines We Can't Live Without

Machines and cloud computing are driving unprecedented improvements in business efficiency. As businesses increase their reliance on machines, the number of machines is growing exponentially.

The future—with service meshes, microservices, containers and functions all operating across clouds—will bring many more machine identities. To communicate securely, each machine needs a unique identity that is trusted, meets policy, and protects from attack. However, organizations' abilities to protect these machine identities is simply not keeping up with the pace of their evolution.

Taming the Chaos: Common Services

Businesses operating in a multi-cloud model require a set of standard, common services to achieve consistency, agility, and speed. As the implications of the cloud operating model impact teams across infrastructure, security, networking, and applications, we see a repeating pattern amongst enterprises of relying on cloud- and environment-agnostic platform services to deliver the dynamic infrastructure necessary for secure application delivery.

Venafi and HashiCorp together, aim to provide a consistent platform that enables teams to move fast and safely, while providing freedom of choice and agility over where applications run. It's a proven blueprint for success.

Protecting Machine Identities

The Importance of Machine Identities

Machine identities, such as X.509 certificates, have always proven troublesome for security teams. For one thing, cybersecurity is not a core skill of application and operation teams. Meanwhile, security teams too often struggle to preserve machine identities using an inefficient hodgepodge of spreadsheets and interfaces from internal PKIs and certificate authorities (CAs) that fail to provide visibility across their IT environments.

Security teams also must worry about whether application and operations team might make mistakes or ignore policy. This has led to unknowns that turn into costly certificate-related outages, such as those seen at LinkedIn, O2, Softbank, Microsoft Azure and many others. In addition, massive data breaches like that of Equifax in 2017 are often made worse by untracked, expiring certificates blind to attack.

The shift to containers, microservices and infrastructure as code also introduces new challenges specific to machine identities. The dynamic nature of infrastructure complicates the task of uniquely identifying, authorizing and securing communication between physical and virtual machines. The rapid deployment, change and revocation of their identities exponentially increases the challenge of keeping communication between cloud workloads secure.

Because machines are now used to control nearly every aspect of our global digital economy, the need to create, install, rapidly assess and ensure the integrity of communications between machines is critical and must be able to scale instantly. Most organizations simply do not have the technology or automation needed to accurately monitor and protect the vast number of machines identities businesses now require.

What Security Teams Need: Real-Time Policy Enforcement and Visibility

Security teams must know what to trust and what not to trust *at all times* to effectively protect machine identities in dynamic environments. As a result, smart policy enforcement must be automated and embedded into the tools used by application development teams. By shifting machine identity processes left into the pre-production phase and hooking directly into automated DevOps workflows, security teams can regain control over X.509 certificates in fully automated environments.

PAST VS. FUTURE: STRATEGIES FOR SECURITY TEAMS

	PAST	FUTURE
VISIBILITY	Scanning	Real-Time
INTELLIGENCE	Spreadsheets / Nothing	Smart Policy
AUTOMATION	Clicks	APIs / Open Source

What DevOps Teams Need: A Catalog of Common Services

Approaches to software development have evolved dramatically over the past decade. With this shift, processes for X.509 certificates must also evolve. It is important that these processes evolve from human-based processes to those driven, maintained and executed automatically using code.

Developers are now the first line of defense and have the shared responsibility to uphold the security team's policies. Thus, rather than take a stitch-it-together approach to security, developers should rely on a centralized common service provided by the security team to achieve speed and compliance with enterprise security policies.

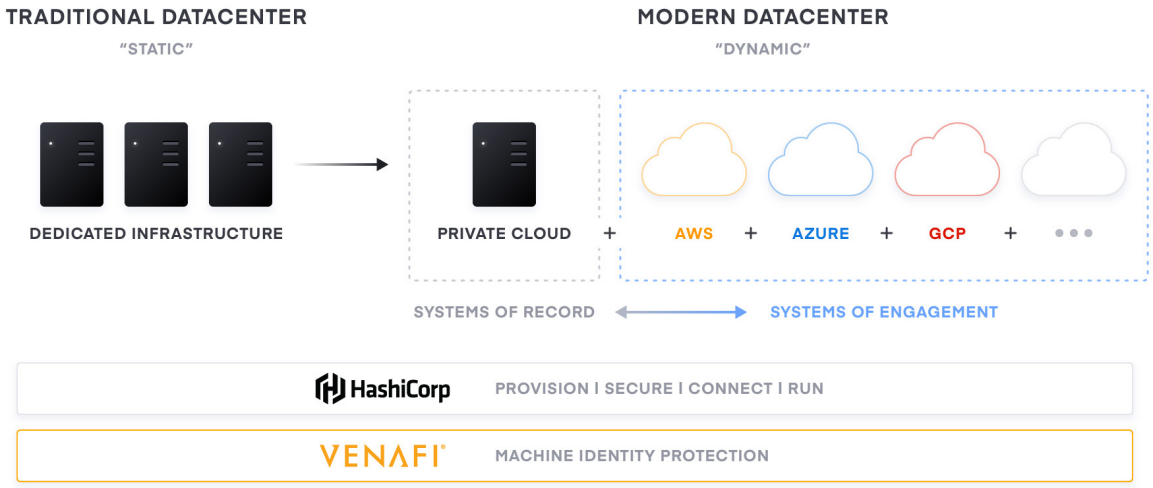
PAST VS. FUTURE: STRATEGIES FOR DEVOPS TEAMS

	PAST	FUTURE
VISIBILITY	Documented By Report	Documented By Code
INTELLIGENCE	Documented By Process	Coded In API
AUTOMATION	Provision Outside Code	Coded In Pipeline

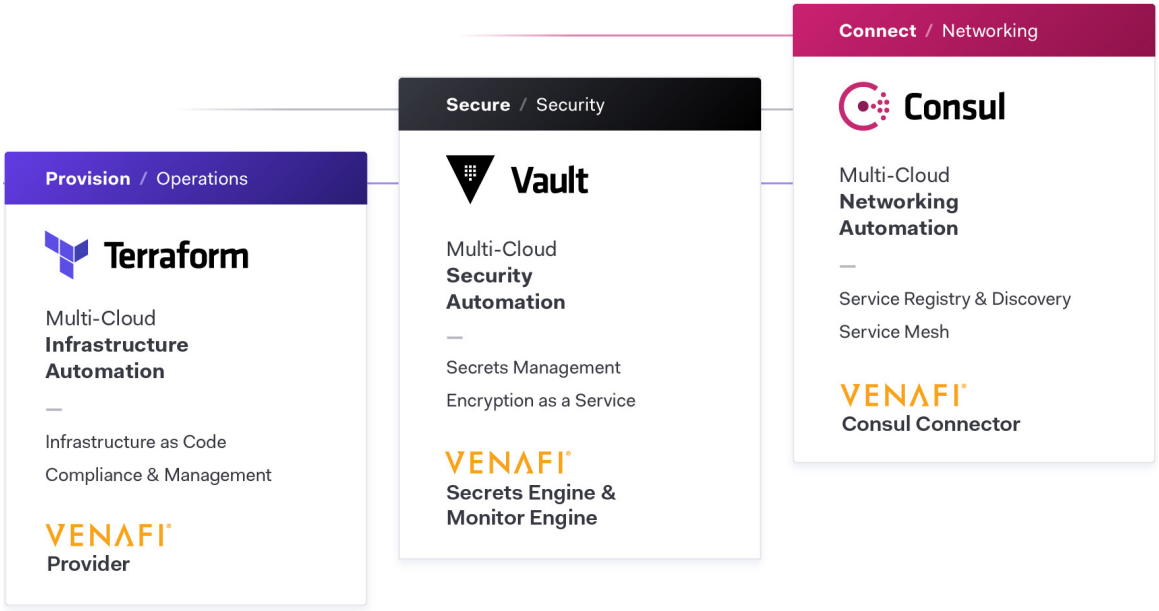
Blueprint for the Cloud Operating Model: HashiCorp and Venafi

Together, Venafi and HashiCorp deliver the platforms that empower DevOps and security teams to be successful in this multi-cloud generation. Infrastructure and applications can be built, secured and connected safely and at the speed today's DevOps teams expect. Application development teams no longer have to be concerned with the details of X.509 certificates when consuming a common service from the security team using Venafi. Security teams maintain smart policy enforcement so their compliance and threat protection responsibilities to the business and customers are always met.

As a common service across clouds, HashiCorp delivers consistent workflows to provision, secure, connect, and run any infrastructure for any application. Venafi integrates with HashiCorp to protect machine identities by delivering visibility, intelligence and automation for X.509 certificates. Venafi also seamlessly makes available a rich ecosystem of more than 40 certificate authorities from within HashiCorp modules, making both private and public trust certificates easy to consume.



HashiCorp and Venafi: Common Services Across Clouds

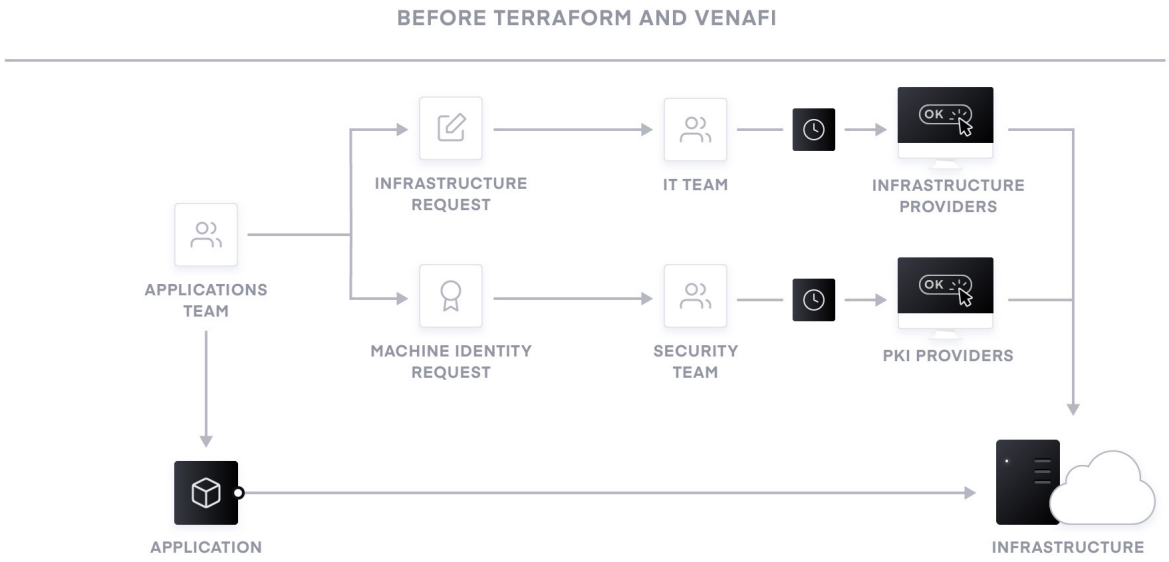


The Cloud Operating Model: How HashiCorp and Venafi support the model together

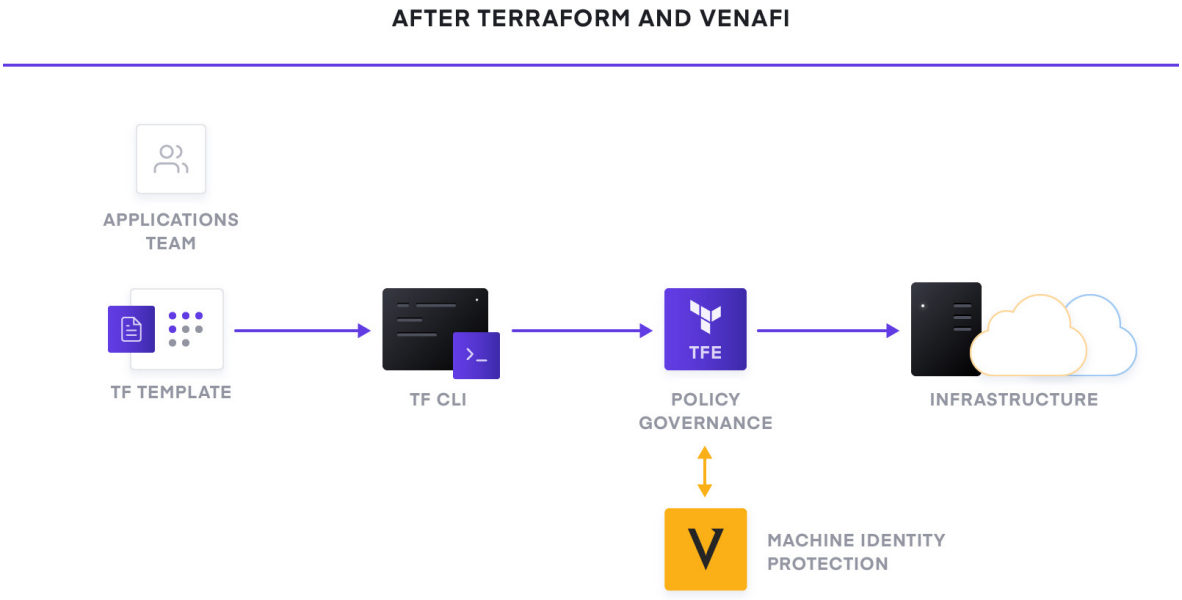
Build: Terraform + Venafi

Automate building infrastructure as code. Deliver machine identities on demand.

The foundation for adopting the cloud is infrastructure provisioning. HashiCorp Terraform is the world's most widely used multi-cloud provisioning solution and can be used to provision infrastructure for any application using an array of providers for any target platform.

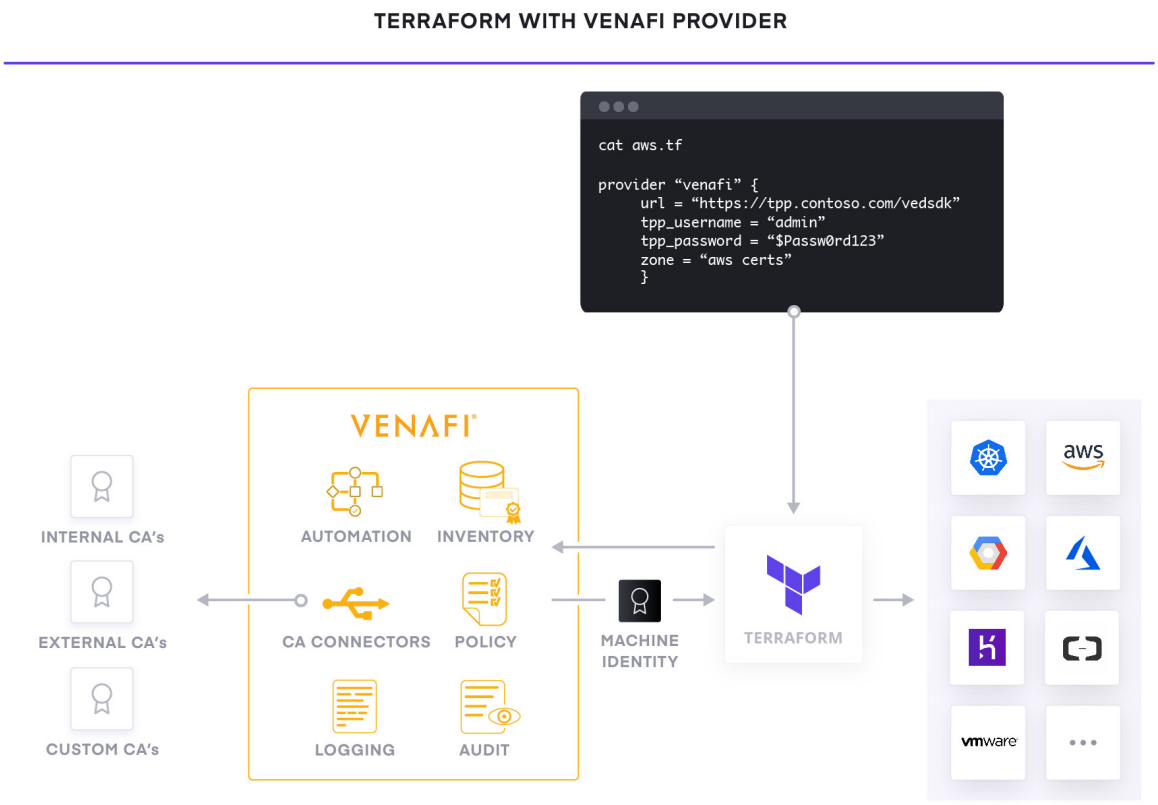


Before Terraform and Venafi: Infrastructure Provisioning and X.509 Certificate Issuance



After Terraform and Venafi: Infrastructure Provisioning and X.509 Certificate Issuance

To achieve shared services for infrastructure provisioning across clouds, teams need to define in code reproducible infrastructure as code practices. Used in combination with Venafi, Terraform builds infrastructure with machine identities that fit the smart policies and compliance required by security. This speeds DevOps teams' performance with a fast, easy, and consistent service consumed in code.



Venafi Provider for Terraform: Automating Smart Policy Enforcement for X.509 Certificates

Without policy as code, organizations resort to using a ticket-based review process to approve changes. This results in developers waiting weeks or longer to provision infrastructure, including machine identities, and becomes a bottleneck. This encourages developers to source machine identities outside of enterprise security controls. Not only does this introduce compliance and security risks (because machine identities expire and often go untracked), it can also introduce debilitating outages from certificate expirations.

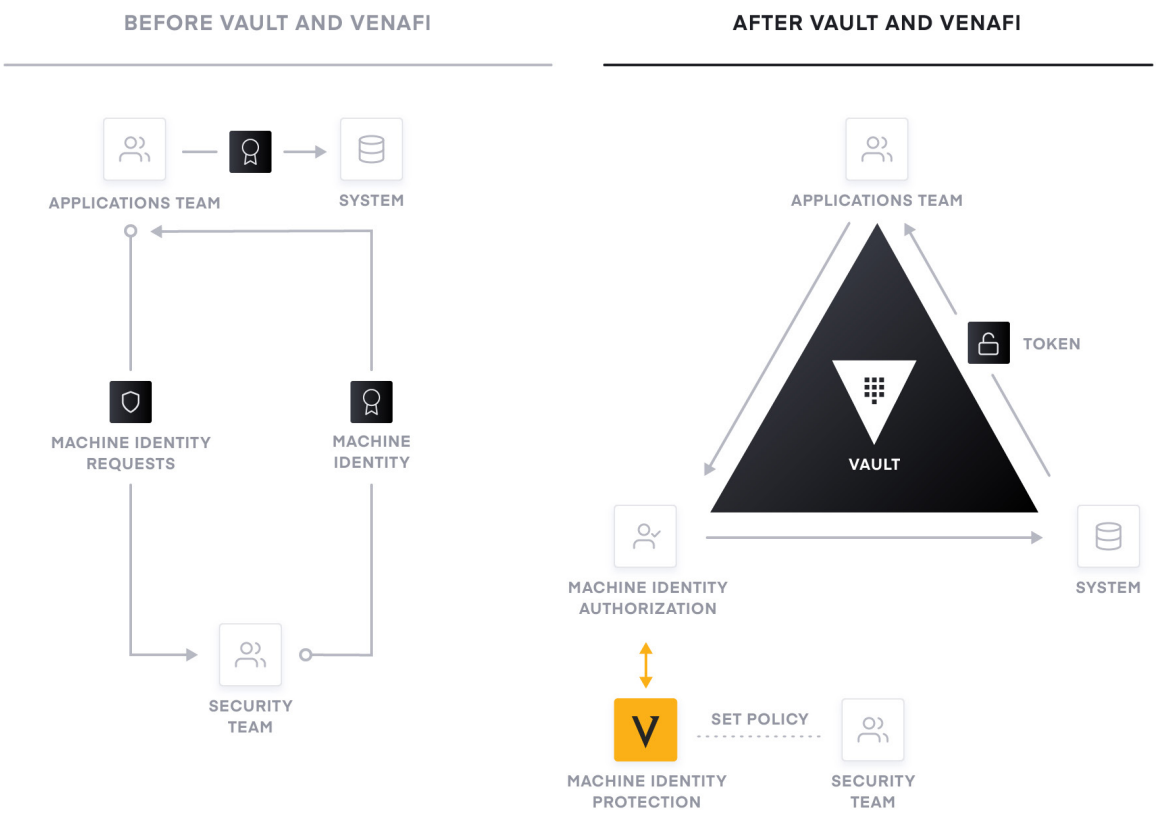
By defining machine identities and policies in code, their request, issuance, and lifecycle are always from approved PKI sources, thus security teams can be confident they are able to continuously enforce policy and maintain visibility.

Secure: Vault + Venafi

Provide developers easy and secure access to secrets. Enable security oversight.
Dynamic cloud infrastructure means a shift from host-based identity to machine-based identity, with low- or zero-trust networks across multiple clouds without a clear network perimeter. In the traditional security world, we assumed that internal networks were high trust, which resulted in a hard shell and soft interior. With the modern "zero trust" approach, it is important to harden the inside as well. This requires that machines be explicitly authenticated and authorized before they can fetch secrets and perform sensitive operations, while being tightly audited.

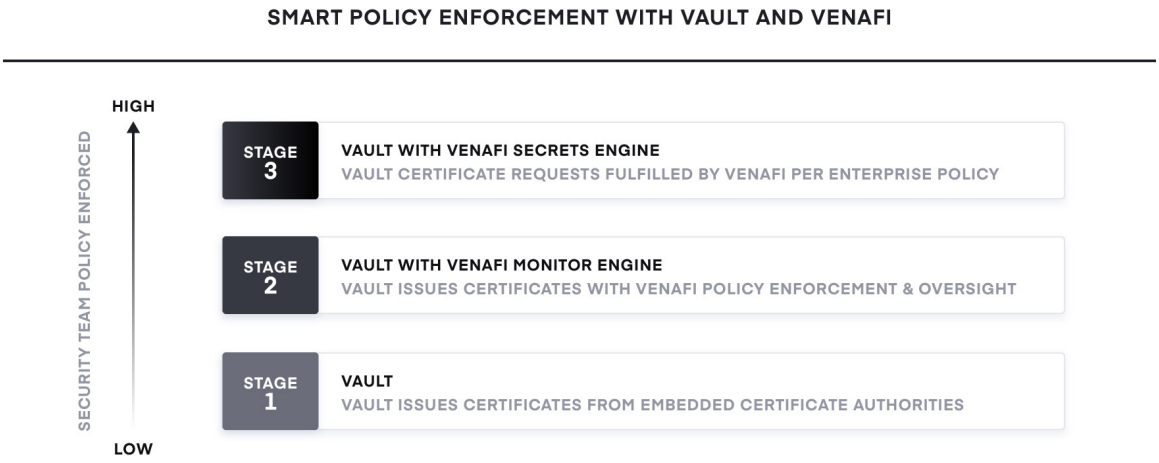
HashiCorp Vault enables teams to securely store and tightly control access to tokens, passwords, certificates, and encryption keys needed to protect machines. This provides a comprehensive secrets management solution. Vault uses policies to codify how applications authenticate, which credentials they are authorized to use, and how auditing should be performed.

Vault also can act like a CA, to provide dynamic short-lived certificates to secure communications with TLS. This is especially useful in low-latency, high-throughput machine identity use cases.



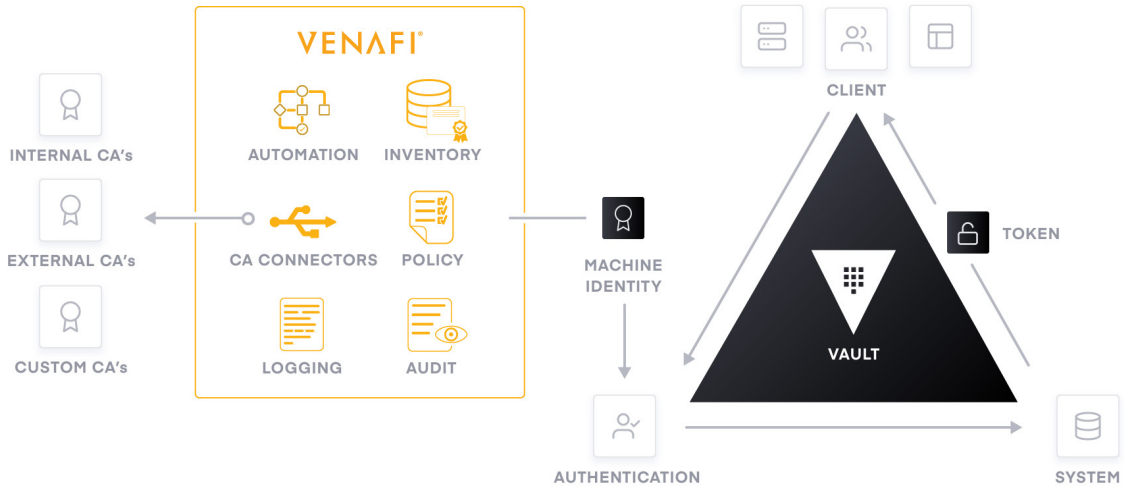
Before and After Vault and Venafi: X.509 Certificate Issuance

For security teams, Vault provides the opportunity to implement policy without getting in the way or slowing down DevOps. However, without centralized visibility and control of the policies used across all Vault instances, autonomous issuance of X.509 certificates is often considered higher risk. As illustrated in the Smart Policy Enforcement with Vault and Venafi diagram below, using the Secrets Engines from Venafi in combination with Vault allows security teams to achieve the desired risk level and smart policy enforcement for all applications required without slowing down DevOps.



Smart Policy Enforcement: Using Vault and Venafi for X.509 Certificates

Venafi and HashiCorp enable teams to have the right level of risk, autonomy and performance without ever sacrificing risk or policy compliance.



Venafi Secrets Engine for Vault: Automating Smart Policy Enforcement for X.509 Certificates

Venafi Secrets Engine for Vault

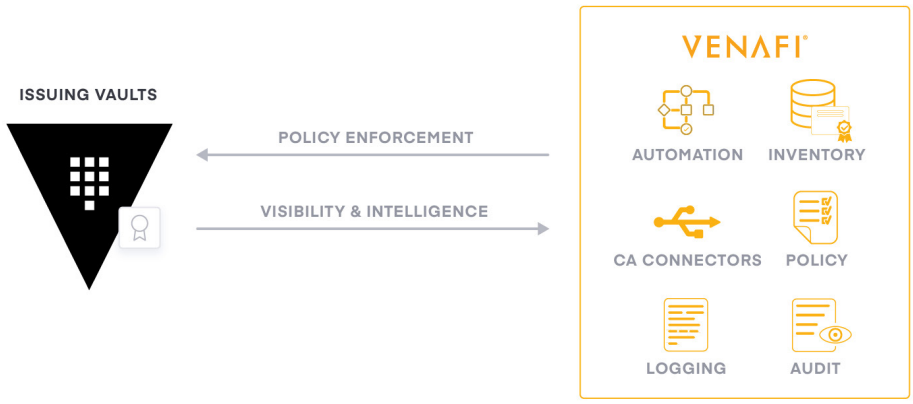
The Venafi Secrets Engine for Vault makes it easy and fast for DevOps teams to obtain X.509 certificates using the Machine Identity Protection service operated by the organization's security team.

- Provides native Vault PKI engine connected to 40-plus CAs
- Delivers publicly trusted certificates without custom coding for CAs such as DigiCert, Entrust and GlobalSign
- Eliminates complexity and errors by automating the certificate lifecycle
- Enforces security team policies within the native Vault workflow
- Gives security teams centralized visibility and auditability
- Enables consistent multi-cloud operations

Venafi Monitor Engine for Vault

The Venafi Monitor Engine for Vault allows security teams to seamlessly define roles within Vault for smart policy enforcement (e.g. no wildcards, hash algorithm, key length, domain names) seamlessly. This enables developers to use native Vault commands for requesting certificates as they normally would while fully complying with corporate security and audit policies with no latency.

- Enforces security team policies within the native Vault workflow
- Forwards all certificates issued by the Vault local CA to Venafi for visibility and auditing
- Gives security teams centralized visibility and auditability
- Eliminates complexity and errors by automating the certificate lifecycle
- Enables consistent multi-cloud operations



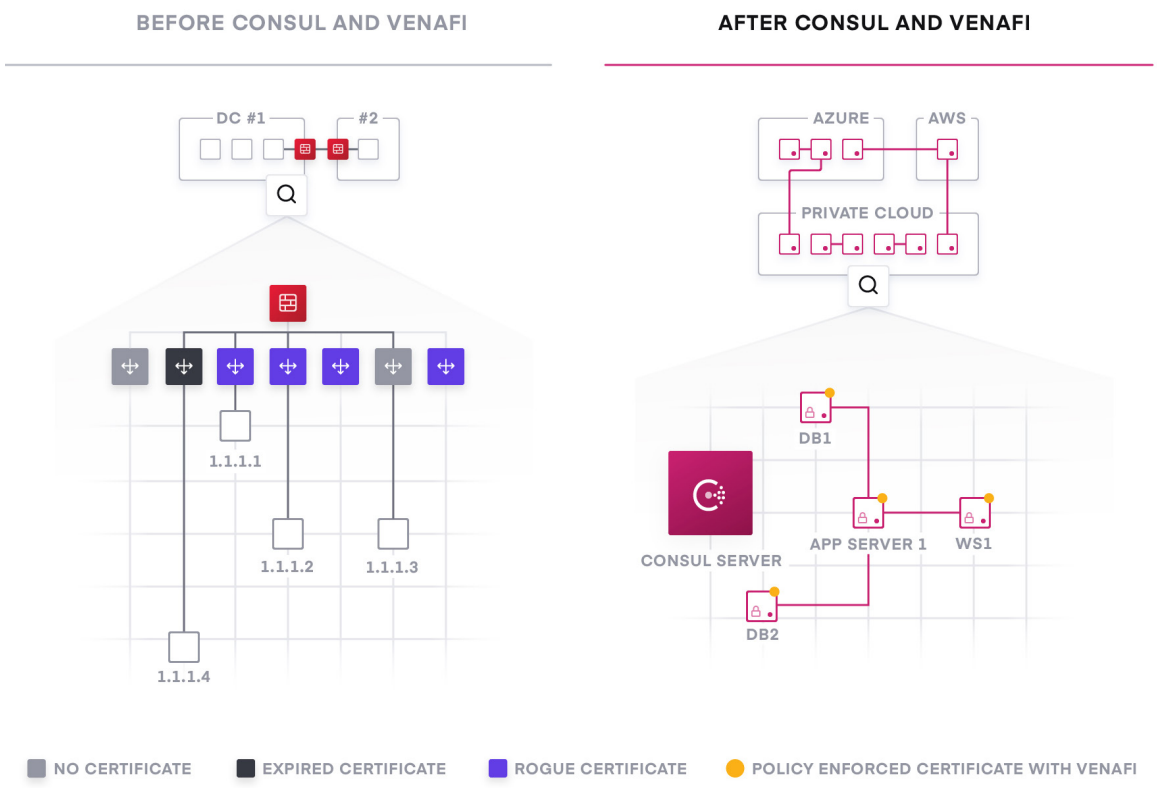
Venafi Monitor Engine for Vault: Smart Policy Enforcement for X.509 Certificates Issued by Vault

Connect: Consul + Venafi

Secure multi-cloud networking at machine speed made easy for DevOps. New levels of protection for security.

A multi-cloud service networking platform to connect and secure services across any runtime platform and public or private cloud.

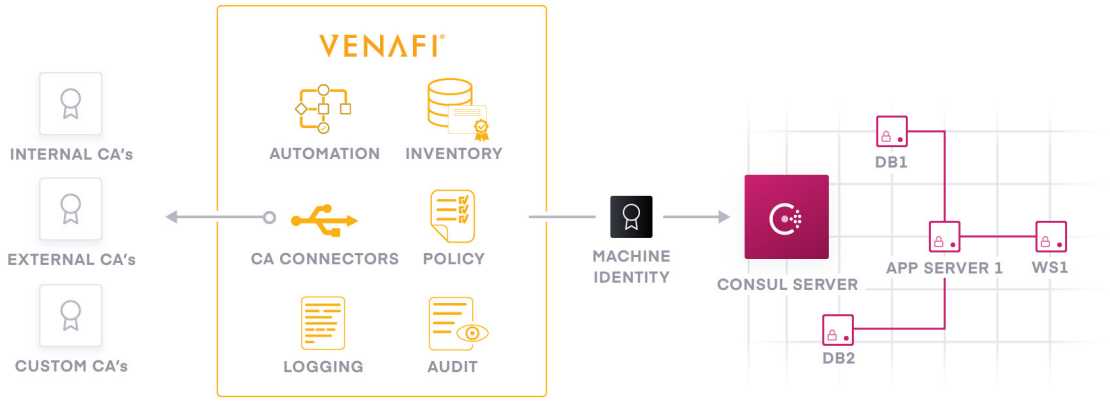
The challenges of networking in the cloud often are one of the most difficult aspects of adopting the cloud operating model for enterprises. The combination of dynamic IP addresses, a significant growth in east-west traffic as the microservices pattern is adopted, and the lack of a clear network perimeter is a formidable challenge. This creates a new attack surface.



Before and After Consul and Venafi: Infrastructure Modernization and X.509 Certificates

HashiCorp Consul provides a distributed service mesh to connect, secure, and configure services across any runtime platform and cloud. Consul provides an API-driven control plane, which integrates with proxies such as Envoy, HAProxy, and Nginx for the data plane. This allows critical functionality like naming, segmentation and authorization, as well as routing to be handled by proxies at the edge rather than using centralized middleware.

Consul enables fine-grained service segmentation to secure service-to-service communication with automatic TLS encryption and identity-based authorization. Consul can be integrated with Vault for machine identities. Consul works directly with Venafi to request X.509 certificates or can consume certificates from Vault.



Venafi Consul Connector: Smart Policy Enforcement for X.509 Certificates

In all cases, only trusted machine identities are used which delivers a new level of protection for applications that was not previously possible. Security teams also get complete visibility and intelligence over which machines are secured with approved X.509 certificates.

Build Your Vision

Venafi and HashiCorp provide you a proven blueprint for the future today. Used worldwide by the Global 5000, the solutions enable DevOps to go fast and safely, while letting security maintain smart policy enforcement without slowing down development.

For Security Teams

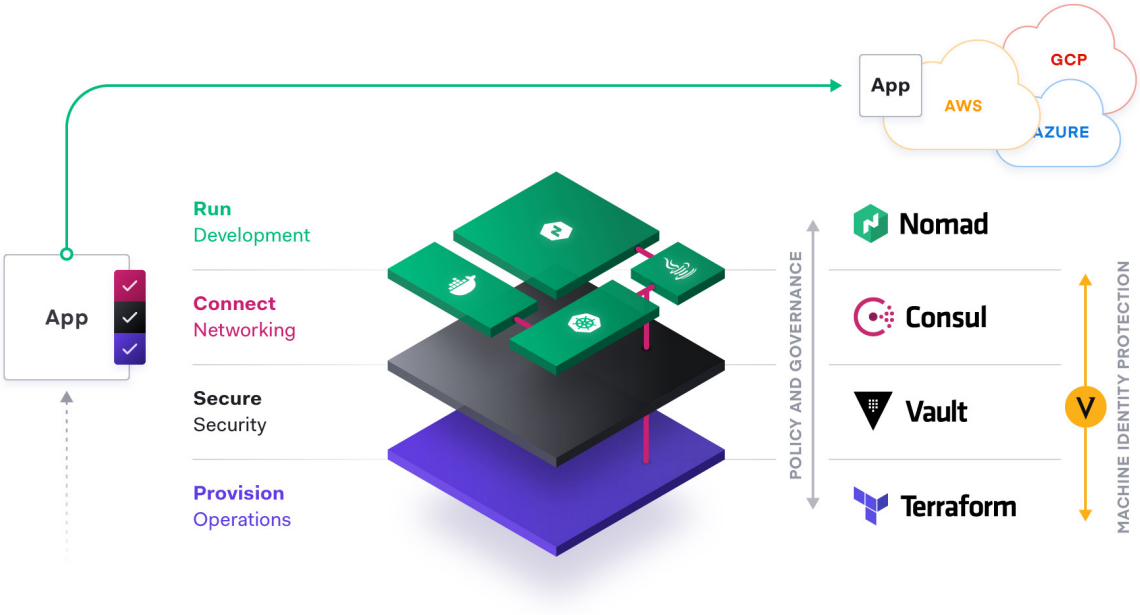
The combination of HashiCorp and Venafi now gives security teams confidence that their business is safe in the multi-cloud generation. By providing a service with Venafi that DevOps teams consume through native HashiCorp integrations, security teams:

- Eliminate errors by supporting Terraform including certificate expirations and outages
- Get smart policy enforcement with Vault everywhere developers need to consume X.509 certificates
- Improve visibility and security with Consul at machine speed that delivers zero-trust protection

For DevOps Teams

Obtaining and using machine identities like X.509 TLS keys and certificates has, up until now, been a necessary but cumbersome requirement. Security teams using Venafi can now provide an enterprise service across private and public clouds. By using HashiCorp with Venafi, DevOps can now:

- Build infrastructure as code with Terraform that is consistent and ready for change
- Get the flexibility of Vault using different secrets engines based on use case
- Go faster with Consul to connect applications while delivering the highest level of application security that legacy networks cannot



Blueprint for the Cloud Operating Model: Protecting Machine Identities with HashiCorp and Venafi


HashiCorp