HashiCorp

WHITE PAPER

Security Lifecycle Management with the HashiCorp Cloud Platform

Table of contents

Executive summary

According to HashiCorp's 2024 State of Cloud Strategy Survey, security is the number one factor highly cloud-mature organizations use to assess cloud success — and the number one benefit they say they get from their cloud program. Security was also the most-cited benefit resulting from the cloud strategy at high-maturity organizations.

To achieve high cloud maturity, today's multi- and hybrid-cloud environments call for a new approach to both Infrastructure Lifecycle Management (ILM) and Security Lifecycle Management (SLM). ILM is the process of building, deploying, and managing the infrastructure that underpins cloud applications. SLM is about how organizations manage their most sensitive data, from creation to expiration. Your approach to SLM should be built on a zero trust, identity-based access architecture, enabling teams to continuously protect credentials and other secrets, inspect their digital estate for unsecured secrets, and connect authorized machines, services, and people.

At the majority of companies adopting cloud infrastructure, we see ILM and SLM taking shape across three stages of maturity:

- **Stage 1 - Adopting:** The adopting phase is when organizations gain familiarity with the cloud and provision their first resources. They also focus on centrally managing static secrets and credentials, ensuring they appropriately authenticate and authorize access to all resources, and leverage tools and processes to gain better visibility into the security of their applications and infrastructure. Results include better control and visibility of secrets to reduce the risk of downtime and breaches.
- **Stage 2 - Standardizing:** IBy the time organizations reach the standardizing stage, they have gained familiarity with provisioning and securing cloud resources. However, they soon discover that without guardrails in place, security and compliance issues start to emerge. This discovery highlights the need to establish a consistent approach to securing infrastructure and applications in addition to effectively enforcing policies across the organization. Results from standardizing include overall reduction in person-hours and associated costs from automating manual secret and credential management tasks.
- **Stage 3 - Scaling:** In this final stage, organizations scale out security lifecycle management capabilities to private datacenters in addition to multiple cloud environments. Scaling out can also include automating more complex processes such as PKI certificate and key management and enabling advanced data protection to meet industry or government requirements. Results from scaling include reduced complexity and improved security when scaling out into multi- and hybrid-cloud operations.

This paper shows how organizations can leverage SLM to reduce their attack surface area as they progress through three stages of cloud adoption maturity: **adopting**, **standardizing**, and **scaling**. And it lays out a blueprint for successful Security Lifecycle Management (SLM) with the **Infrastructure Cloud**, an integrated portfolio of products powered by the **HashiCorp Cloud Platform** (HCP).

Why the cloud makes it hard to manage security

As organizations accelerate their adoption of cloud infrastructure and applications, they face increased security risks. Securing infrastructure with static perimeters and IP addresses is no longer adequate in modern dynamic, distributed cloud and on-premises environments. The cloud also makes it easier for developers to rapidly create and deploy applications, which can complicate efforts to maintain visibility and control, not to mention enforce security best practices.

The focus on fast, agile development in the cloud often leads to **secret sprawl**, providing over-access to resources, and exposure of sensitive data such as personally identifiable information (PII) or payment card information (PCI) due to a lack of visibility, lack of control, and long-lived secrets. (A secret can be anything that provides access to a system by authenticating humans or machines and authorizing them to perform actions such as reading and writing data from a database or gaining access to secure developer resources.)

When we say “secret sprawl”, we’re really talking about the wide distribution of secrets and the difficulty of tracking and managing them. A classic example is a database username and password hard-coded into the source code of an application.

In the case of providing human access to secure resources, users are often given more access than they need because it can be challenging to manage granular permissions for large numbers of users. VPNs are commonly used to provide remote user access to infrastructure resources. However, securing this type of access remains a concern because managing credentials to target resources is cumbersome and principles of least privilege are not typically enforced. Challenges in managing credentials for secure access also apply to communication between application services.

The three categories of cloud security risks

Cloud security risks fall into three main categories:

Lack of visibility

With so many places for secrets to hide, it can be difficult to keep track of them all. One team might be using a cloud-native secrets manager and another team might store secrets in a GitHub repo, or in a Wiki because it's faster and easier. This leads to lack of visibility in terms of what secrets might be exposed and how big the blast radius of that exposure might be.

Lack of control

Without central control of secrets, credentials, and sensitive data, breaches can be impossible to contain. If least-privileged access is not enforced, then someone with too much access can do a lot of harm. If a database username and password gets exposed, how do you know where that username and password came from? Without central visibility and control, you may not have the necessary data from access logs or other sources to identify and remediate the issue.

Long-lived secrets

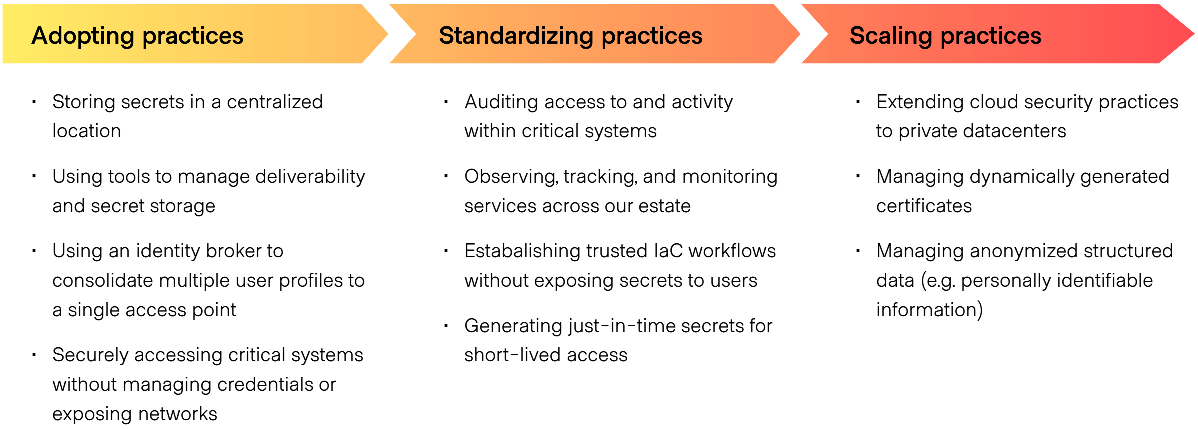
Even when secrets and credentials are properly stored, they are often static and long-lived. The longer secrets and credentials remain in use, the more likely they are to be compromised.

The result: costly breaches, downtime, and lost revenue

To address overly broad access, secret sprawl, and long-lived credentials, organizations need a new approach to Security Lifecycle Management.

A maturity-based blueprint for cloud success

Addressing today's security challenges requires a modern, holistic approach to secrets management across people, processes, and tools. Over the last decade, HashiCorp has helped thousands of customers mature their use of the cloud and deliver on their business objectives. This work has revealed a consistent three-stage blueprint for success, in this case focused on SLM.



Adopting practices

- Storing secrets in a centralized location
- Using tools to manage deliverability and secret storage
- Using an identity broker to consolidate multiple user profiles to a single access point
- Securely accessing critical systems without managing credentials or exposing networks

Standardizing practices

- Auditing access to and activity within critical systems
- Observing, tracking, and monitoring services across our estate
- Estabalishing trusted IaC workflows without exposing secrets to users
- Generating just-in-time secrets for short-lived access

Scaling practices

- Extending cloud security practices to private datacenters
- Managing dynamically generated certificates
- Managing anonymized structured data (e.g. personally identifiable information)

This blueprint gives organizations a maturity model to benchmark where they stand in their cloud journey, identify the relevant use cases, and determine next steps toward modernizing their approach to Security Lifecycle Management.

The stages of cloud security lifecycle management

Security Lifecycle Management involves protecting secrets, certificates, and other credentials, inspecting your digital estate for unsecured credentials, and securely connecting authorized machines, services, and people. The process starts with the creation of a secret, perhaps for something as simple as enabling an application to talk to a database. This secret needs to be rotated regularly, and many organizations spend thousands of hours manually rotating secrets. Other organizations may not have the resources to rotate the secrets often enough, or even rotate them at all. And, of course, this newly rotated secret might require a refresh of the associated infrastructure to pick up the change, which emphasizes the interconnected nature of ILM and SLM. Ultimately, when the associated application is no longer needed and is decommissioned, the secret should be destroyed to reduce the potential attack surface.

Security Lifecycle Management delivered via the HashiCorp Cloud Platform is designed to address the challenges of each stage of the secret lifecycle. HashiCorp offers a portfolio of SLM products managed on HCP that enable a unified infrastructure workflow including HashiCorp Vault, Vault Radar, Boundary, and Consul. Each of these products addresses a specific challenge, and together they form a comprehensive workflow for addressing security needs across all stages of infrastructure and application deployment:

- **Vault for secrets management:** Provides an identity-based approach to security that automatically authenticates and authorizes human or machine access to secrets and other sensitive data.
- **Vault Radar for secret scanning:** Enables the automated detection and identification of unmanaged secrets in your code, collaboration tools, and other common environments so that security teams can take appropriate actions to remediate issues.
- **Boundary for remote user access:** Built for the cloud, Boundary's modern approach to privileged access management uses identity-driven controls to secure user access across dynamic environments.
- **Consul for service networking:** Offers an identity-based approach to service networking for service discovery, secure service-to-service communication, and network automation across multiple cloud and runtime environments.

To truly understand Security Lifecycle Management, you need to look across all three stages of cloud maturity: **adopting**, **standardizing**, and **scaling**. The remainder of this paper will address use cases at each step and explore specific capabilities offered by the HashiCorp SLM portfolio that help organizations establish a successful and secure cloud program.

Stage 1 - Adopting

In the adopting phase, resource provisioning is still very ad hoc, as various teams take different approaches and use different tools. This variability leads to an inconsistent approach to SLM, so organizations in this phase should focus on centrally managing static secrets and credentials, authenticating and authorizing access to resources, and gaining better visibility into the security of their applications and infrastructure.

Manage static secrets

In the adopting stage, organizations start by protecting the static — and often most vulnerable — parts of their infrastructure. Stolen credentials account for 77% of web application attacks, according to the **Verizon 2024 Data Breach Investigations Report**. Gaining control over static credentials and secrets means centrally managing them and protecting them through least-privileged access policies and encryption. Individual teams within an organization begin by making **Vault** their system of record for generating and managing static secrets.

Organizations that use multiple different secret repositories and don't want to alter their DevOps tools and workflows can centralize their secrets management by using **HCP Vault Secrets** to centrally sync and manage their key-value (KV) secrets with the native repositories they're already using. To reduce the risk of long-lived static credentials, organizations can also enable **auto-rotation** of their static secrets.

It's also important at this stage to implement least-privileged access when users connect to secure or sensitive resources. Remote users often manually handle and store credentials in insecure locations, which can lead to breaches. To provide a more secure and streamlined cloud-based option, **Boundary enables organizations to centrally store, access, and deploy key-value credentials** across applications, systems, and infrastructure.

Authenticate and authorize

Operating in cloud and distributed environments poses a new challenge when it comes to granting access to secure data and environments. Traditionally, this was done with dedicated servers, static IP addresses, and a clear network perimeter. In the cloud, organizations deal with ephemeral and elastic pools of infrastructure with dynamic IP addresses and no clear perimeter. That's why modern cloud and distributed environments require identity-based access.

HCP provides secure access to secrets, systems, and data with trusted identities. In the adopting stage, organizations use Vault, Boundary, and Consul to ensure proper access and control for human access and control, machine-to-machine access, and human-to-machine access. One way to enforce least-privileged access is through integrations with popular identity providers such as cloud IAM platforms like Ping, Okta, Microsoft Entra ID, Kubernetes, and Active Directory. Both Vault and Boundary support this type of IAM provider integration.

Many organizations distribute and manage SSH keys, VPN credentials, and bastion hosts, which leads to secret sprawl and increases the risk of a breach where attackers gain access to entire networks and systems. **Boundary** addresses this by streamlining how end users access infrastructure resources such as Linux/Windows hosts via SSH or RDP, Kubernetes clusters using kubectl, web applications, or databases. Boundary enforces least-privileged access and handles credentials on behalf of the end user. Credentials may be stored within Boundary and brokered to the end user for each session. Access into the network is secure and proxied, dramatically shrinking the attack surface. The core Boundary workflow, Transparent Sessions, simplifies end-user access.

Consul service mesh provides secure machine-to-machine access with automated authorization and authentication between network services on any platform or runtime, significantly improving network security. Rather than relying on network firewalls that control access based on ephemeral IP addresses, Consul authorizes service-to-service communication based on an identity. All communication between services is encrypted. Offloading these functions onto Consul not only enhances network security and enforces zero trust principles, it also reduces the effort required by developers and platform security operators to provide the same security measures.

To further secure access control, roles can be created with assigned policies to govern access and enable least-privileged security principles.

Gain visibility

Visibility is key in distributed cloud environments so organizations can monitor and maintain secure operations, even in the adopting stage. HashiCorp SLM capabilities provide the ability to internally track and integrate with third-party platforms to ensure proper lifecycle management.

Vault provides rich operational telemetry metrics that can be consumed by popular solutions for monitoring and alerting on key operational conditions and audit devices for logging each Vault request and response. Popular tool integrations include Splunk, Datadog, and Grafana. Using the Vault telemetry and audit device features in combination with metrics and log data can provide invaluable insight into operations and usage.

Boundary provides visibility and management of end-user sessions. Administrators have a full view and history of users and can terminate questionable sessions on demand. Boundary also includes search and filter capabilities to easily navigate and locate a resource out of hundreds or thousands of potential sessions, users, targets, and more.

Consul's integration with existing system-of-record tools helps improve visibility. In the adoption phase, you enable service discovery to let your applications dynamically locate and reach services registered to Consul. You can monitor health and IP address changes for each service directly from the Consul UI. Consul also integrates with Vault as the identity broker for service authentication across clouds, or to leverage features like Vault PKI or Kubernetes secrets management.

Lastly, it's important to understand the scope of your vulnerability from unsecured secrets. **Vault Radar** automates the detection and identification of unmanaged secrets in your code. It continuously scans in real-time for:

- Secrets
- Personally identifiable information (PII)
- Non-inclusive language (NIL)

Once the scanning completes, you can see the results in a dashboard with associated locations, owners, and risk severity to help remediate the issues.

Expected results: Centralizing secret and credential management in a secure location in addition to secret scanning should reduce the number of secrets and credentials in unsecured locations. This should in turn reduce the potential for breaches, application downtime, and lost revenue. Enforcement and enablement of access using identity-based authentication for least-privileged access to sensitive data and resources can further strengthen the organization's security posture. Better visibility provided by telemetry data and monitoring tools enables proactive security lifecycle management.

Stage 2 - Standardizing

The standardizing stage of SLM is all about enabling secrets management, compliance, and continuity across the entire organization. To successfully achieve this standardization, automation is key. When organizations move into the standardizing stage, their priorities center on establishing a cloud platform team and standardizing workflows and tools; their use cases expand to providing dynamic, short-lived secrets to meet more rigid security requirements and establishing networking for secure access between applications. The idea is to reduce the time it takes to manage secrets and credentials while lowering the risk of breach from long-lived static secrets and credentials.

Automate secrets management

HCP Vault Secrets provides two ways to automate secrets management: **auto-rotation of secrets** and **creation of dynamic secrets**. Generated on-demand, dynamic secrets don't exist until they are needed, so there is less risk of someone stealing them or another client using them. Vault and HCP Vault Dedicated enable the generation and management of dynamic secrets through the many secrets engines that support **dynamic secrets**, including **databases**, cloud service providers (**AWS**, **Microsoft Azure**, **Google Cloud**), **LDAP**, and certificates (**PKI**, **SSH**).

The standardizing stage is also when organizations modernize the way they manage secrets across all applications, including legacy applications. **The HashiCorp Vault Agent** can modernize legacy applications by enabling the same type of secret automation used with more modern applications. Organizations running containerized applications use the **Vault Kubernetes Secrets Engine** to generate dynamic credentials used to access Kubernetes. Vault can also be used to centrally manage the secrets of containerized applications via the **Vault CSI provider**, **Vault agent sidecar** injector, or by using the **Vault Secrets Operator** (VSO).

To further automate and standardize human-to-machine access, Boundary provides modern privileged access management (PAM) workflows with automated privileged access and credential injection. These capabilities ensure users can access only the resources that they are authorized to access (least-privileged access) without exposing credentials. Furthermore, Boundary integrates with Vault secrets engines to generate short-lived dynamic credentials that are injected into sessions on behalf of end users, resulting in passwordless access.

Ensure compliance

In the standardizing phase of cloud adoption, it's imperative that teams across the organization consistently ensure security compliance. Vault Radar is used in the adopting stage to scan repositories, find unsecured secrets, and then help users remediate them.

In the standardizing stage, organizations proactively prevent secret sprawl by configuring automated workflows to detect and prevent unsecured secrets and sensitive data from getting into the wild. Vault Radar supports real-time discovery of secrets at commit time. One example of this capability is the ability to **configure webhooks** so that when developers commit code, the webhook notifies Vault Radar, which immediately runs scans to discover whether new secrets have been committed. **Automated scans can also be run against CI/CD pipelines** as part of a CI workflow leveraging tools like GitHub Actions or for **scanning pull requests or branch changes**.

Vault Radar will alert users to any sensitive data found in the pull request. To help with remediating unsecured secrets, the alert includes details on what type of secret was found and where. With support for **integrating with collaboration platforms like Slack**, users can also receive real-time notifications when someone tries to commit or deploy a secret, then can click a link in the message to go directly to the source and investigate.

Access controls are typically enhanced in the standardizing stage across SLM products. While some organizations begin to use Vault namespaces during the adopting stage, it's more commonly implemented as security standardization moves across the organization. **Namespaces** enable the creation of isolated "Vaults within a Vault" that let teams manage their own policies, secrets, and identities. By configuring namespaces, teams can:

- Isolate tenant environments for security and compliance
- Enforce organizational compliance across isolated teams
- Enable multilevel security and advanced access controls.

Vault also provides the capability to create **control groups**. You can use control groups in your policies to implement the requirement for dual controller authorization. A real-world use case would be using control groups in your policies to implement the requirement for dual controller authorization to meet **GDPR requirements**.

The ability to audit for compliance becomes important as you standardize your cloud operations. This capability is supported in Vault, Boundary, and Consul, providing comprehensive visibility into configuration changes, session metrics, events, logs, and traces. This data can also be exported to popular event monitoring tools such as Prometheus, CloudWatch, DataDog, and Splunk. Boundary provides auditing capabilities via session recording, which gives administrators insight into specific user actions and commands over remote SSH sessions. This helps organizations meet regulatory requirements, deter malicious behavior, and expedite remediation in the event of a breach. Administrators can enable session recording on SSH targets in their Boundary environment, store signed recordings in their Amazon S3 storage bucket, use MinIO to store them in any cloud or on-premises, and replay recordings back within the Boundary admin UI.

Ensure continuity

As organizations begin to standardize on HashiCorp SLM products, the number of users, secrets, and operations naturally increases, increasing the need for a disaster recovery (DR) strategy to protect against catastrophic failure. Vault Enterprise supports multi-datacenter deployment where you can replicate data across datacenters for performance as well as disaster recovery. Vault DR also features failover and failback capabilities to assist in recovery from catastrophic failure of entire clusters.

HCP Vault Dedicated is a fully managed implementation of Vault. HashiCorp operates the infrastructure, so organizations can get up and running quickly and avoid the internal costs of running Vault themselves. HCP Vault Dedicated provides high availability replication of secrets and policies across multiple regions of your cloud service, including secret backends config, auth backends config, audit backends config, and batch tokens. This version of Vault also offers snapshot functionality for the underlying storage to preserve data based on your requirements.

Application and service continuity are standardized at this stage. As multiple teams within the organization standardize on Consul, administrative partitions and namespaces support multi-tenancy by allowing different teams to run autonomously within a single Consul cluster, while also facilitating secure connections between services belonging to respective teams. Teams can test the resiliency of their applications by injecting faults between services to ensure behavior is as expected during failure conditions. Rate limiting is supported on both the control plane and data plane to protect resources from getting overloaded. Similar to service discovery, cluster peering provides automatic service failover across different Consul clusters in any runtime, platform, or cloud.

Expected results: A major benefit of moving into the standardizing stage of SLM is the overall reduction in person-hours and associated costs realized by automating manual secret and credential management tasks. Using dynamic secrets and credentials minimizes their exposure, which further reduces risk and costs from downtime or breaches. Improved efficiency also comes from standardizing tools and processes across the organization, as well as ensuring continuity of system and application operations. Compliance is enhanced with advanced features and automated tools to help meet organizational, business, and government regulations.

Stage 3 - Scaling

The last stage of cloud adoption, scaling, is when organizations apply the principles of a cloud operating model more broadly and authenticate on-premises systems in addition to cloud environments.

Scaling out can also introduce more complexity, creating the need for advanced secret management processes such as PKI certificate and key management. This is because generated certificates can also be distributed and have their lifecycle managed through key-management services. You'll most likely also need advanced data protection capabilities such as **encryption-as-a-service** to encrypt data in transit and at rest across clouds. If you also need to protect sensitive data such as PII, **advanced data protection** capabilities such as data tokenization can transparently protect this information. The following sections describe how these capabilities help reduce complexity:

Manage keys and certificates

Public key infrastructure (PKI) can be complex to configure and manage. Most organizations manage their PKI certificates and keys using a combination of manual processes and multiple tools, which is time-consuming, error-prone, and leads to long-lived certificates, especially in scaled-out distributed environments.

Management needs to be standardized, secure, and automated. The **Vault PKI secrets engine** applies a dynamic-secret approach and can act as an internal private certificate authority (CA) or as a signing intermediary to generate dynamic X.509 certificates. It also supports popular protocols such as **Automated Certificate Management Environment** (ACME) for certificate automation and **Enrollment over Secure Transport** (EST) for managing internet of things (IoT) and other hardware devices. There is no need to use an external registration authority (RA), as Vault provides built-in authentication and authorization mechanisms for this verification functionality. Using Vault to secure and automate the management of certificates lowers risk with shorter TTLs and less chance of human error.

By the time organizations get to the scaling stage, most end up relying on multiple key-management systems when their infrastructure is built on multiple cloud and on-premises platforms. The Vault **Key Management secrets engine** (KMSE) provides a consistent workflow for distribution and lifecycle management of cryptographic keys in various key-management service (KMS) providers. It lets organizations centralize control of their keys in Vault while still taking advantage of cryptographic capabilities native to the KMS providers. KMSE currently supports the three big cloud providers' key management systems: AWS KMS, Azure Key Vault, and Google Cloud's cloud key-management service.

To support advanced encryption for legacy workloads, the **KMIP secrets engine** lets Vault act as a **Key Management Interoperability Protocol** (KMIP) server provider. Because KMIP is a standardized protocol, it can support legacy workloads to enable modern secrets management in private datacenters, including Transparent Database Encryption (TDE), Full Disk Encryption (FDE), virtual volume encryption, multi- and hybrid-cloud key management, securing static credentials, certificate and encryption key management, dynamic database credentials, and more.

Protect sensitive data

To protect sensitive data, many organizations must comply with government regulations or industry standards such as HIPAA and PCI. Vault's **transform secrets engine** supports three advanced data transformation methods to protect sensitive data: format preserving encryption (FPE), tokenization, and data masking.

Vault's **transit secrets engine** is a core feature for protecting sensitive data by providing **encryption as a service**. Organizations use the transit secrets engine to centralize key management and simplify encrypting data in transit and at rest across clouds and datacenters. This relieves the burden of data encryption and decryption from the application developers, and provides several important capabilities:

- Sign and verify data
- Generate hashes and hash-based message authentication code (HMACs) of data
- Act as a source of random bytes

Vault's transit secrets engine handles cryptographic functions on data-in-transit. Vault doesn't store the data sent to the secrets engine, so it can also be viewed as encryption as a service.

Scale out

In the scaling stage, organizations leverage features and capabilities of SLM products in other parts of the digital estate, including private datacenters and private cloud resources. Features like Vault **Workload Identity Federation** (WIF), Boundary dynamic host catalog, and Consul service sameness were developed specifically to help customers expand across multiple environments.

Workload Identity Federation enables secretless configuration for Vault plugins that integrate with external systems supporting WIF, such as AWS, Azure, and Google Cloud. By enabling secretless configuration, organizations reduce security concerns that can come with using long-lived and highly privileged security credentials. By supporting WIF, Vault no longer needs access to highly sensitive root credentials for cloud providers, giving operators a scale-out solution.

As organizations scale their cloud efforts, automation becomes even more critical to ensure proper management. This is true especially in privileged access management tools where one of the fundamental goals is controlling users' access to resources. The number of resources in an environment can easily hit hundreds or thousands. With **dynamic host catalog**, Boundary reduces management overhead by auto-discovering host resources in AWS and Azure. Rather than relying on agents or requiring administrators to manually onboard Amazon EC2 instances or Azure VMs, Boundary can detect these hosts based on tags and automatically add them to the catalog. IP address changes or deleted hosts are automatically detected and updated in the Boundary catalog, lowering maintenance requirements for administrators.

As organizations introduce Boundary to more teams, new use cases with complex and unique network topologies emerge. Many organizations have network enclaves that do not allow inbound access or allow access only through designated networks. Boundary's **multi-hop session** feature lets end users access resources in complex and strict network topologies using reverse-proxy connections across multiple Boundary worker proxies.

One of Consul's core differentiators is its flexibility to run on any platform, runtime, and cloud environment. This allows organizations and teams to secure their network services on the platform that best suits their development teams and offers room to grow into other environments. As organizations execute on multi-cloud strategies, Consul helps organizations securely connect and route services across any public or private cloud environment. This helps application teams securely connect services between on-premises datacenters and public clouds for cloud migration or automated service failover. Features like service sameness and locality-aware routing simplify the configuration process for service failover and keep traffic local until a failover event occurs, reducing management and cloud costs for cross-regional network traffic.

Expected results: Scaling cloud operations out into multi- and hybrid-cloud environments can be extremely complex and risky. In this stage, SLM products help organizations securely manage complex secrets such as keys and certificates across multiple environments in a centralized and automated way. This reduces the costs associated with people, time, and processes. Similarly, sensitive data can be managed across various estates using advanced data protection capabilities for compliance with strict data protection regulations.

Conclusion

The journey to cloud introduces a new paradigm for managing applications, infrastructure and security. This new paradigm presents challenges to organizations that must operate in a new and agile way while still ensuring the security of their environments and resources. These security challenges include a lack of central control and visibility, especially as operations spread beyond a single cloud environment. By taking a staged approach to cloud maturity and leveraging HashiCorp's Security Lifecycle Management capabilities, organizations can accelerate their adoption of cloud infrastructure and applications in a secure and efficient way.

To start implementing Security Lifecycle Management in your organization, **sign up for a free HCP account today**.

Resources

Stage 1 - Adopting

Manage static secrets: Individual teams within an organization start generating and managing static secrets using Vault's KV secret engine for better security and control.

- Generate and manage static secrets with Vault
- Centrally sync and manage key-value (KV) secrets using HCP Vault Secrets
- Use HashiCorp Vault Secrets to configure auto-rotation of static secrets
- Use HCP Boundary to store, access, and deploy static credentials for remote access

Authenticate and authorize: Organizations use Vault, Boundary, and Consul to ensure proper access and control for human access and control, machine-to-machine access and human-to-machine access.

- Use trusted identity providers to enable identity-based access and security
- Use Consul to enable identity based service-to-service communication
- Use Boundary for least-privileged access to secure resources

Gain visibility: Visibility is key in distributed cloud environments in order to monitor and maintain secure operations. Organizations use Vault, Boundary, and Consul to internally track and integrate with third-party platforms to ensure proper lifecycle management.

- Integrate Vault with popular third-party monitoring and alerting solutions to gain operational insights
- Use Boundary for visibility and management of end user remote access sessions
- Integrate your catalog of services with your DNS service to dynamically locate and reach services registered to Consul
- Use HCP Vault Radar to scan your environments and find unsecured secrets and sensitive data

Stage 2 - Standardizing

Automate secrets management: When organizations move into the standardizing stage, their use cases expand to providing dynamic, short-lived secrets to meet more rigid security requirements and establishing networking for secure access between applications.

- Use Vault's dynamic secret capability to automatically generate short-lived, just-in-time secrets for better security
- Use the Vault Agent to modernize legacy applications by enabling the same type of secret automation used with more modern applications
- Use Vault's Kubernetes secrets engine to generate dynamic credentials used to access Kubernetes service accounts
- Leverage Vault dynamic secrets with Boundary to enable more secure human-to-machine connections

Ensure compliance: In the standardizing phase, it's imperative that teams across the organization are aware of and consistently ensuring security compliance.

- Use Vault Radar to prevent secret sprawl by configuring automated workflows
- Ensure secure workflow and access isolation using Vault namespaces
- Create control groups to implement the requirement for dual controller authorization
- Leverage detailed audit logging in Vault, Boundary, and Consul for compliance management
- Use Boundary session recording to meet various regulatory requirements, deter malicious behavior, and expedite remediation in the event of a breach

Ensure continuity: As usage of secret lifecycle management products increases in the standardizing phase, organizations must protect against catastrophic failure of an entire cluster.

- HCP Vault Dedicated provides high-availability replication of secrets and policies across multiple regions of your cloud service
- Use snapshot functionality to preserve Vault data based on your requirements
- Use Admin partitions and namespaces to enable multiple teams to run autonomously within a single Consul cluster

Stage 3 - Scaling

Manage keys and certificates: Most organizations end up relying on multiple key management systems when their infrastructure is built on multiple cloud and on-premises platforms. The challenge is getting better central visibility and control to properly manage things like certificates and the encryption key lifecycle.

- Use Vault to generate and manage PKI certificates
- Enable ACME with the PKI secrets engine
- Use a PKI mount to authenticate EST enabled hardware devices

Protect sensitive data: Many organizations need to meet advanced data security requirements driven by government regulations or industry standards.

- Use Vault's transform secrets engine to protect sensitive data
- Use Vault's key-management secrets engine to enable consistent distribution and lifecycle management of cryptographic keys
- Enable Vault to act as a Key Management Interoperability Protocol (KMIP) server provider
- Enable encryption as a service with Vault's transit secrets engine

Scale out: At this stage, organizations are also extending secrets management workflows into an increasingly wider range of platforms and systems, including private datacenters.

- Enable secretless configuration to integrate with external systems such as AWS, Microsoft Azure, and Google Cloud
- Use Boundary's dynamic host catalog to auto-discover host resources in AWS and Azure
- Use Boundary's multi-hop session to let end users access resources in complex and strict network topologies
- Use Consul to securely connect and route services across any public or private cloud environment

About HashiCorp

HashiCorp is a leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows and create a system of record for automating the cloud: infrastructure provisioning, security, networking, and application deployment. HashiCorp's portfolio of products includes Vagrant™, Packer™, Terraform®, Vault™, Consul®, Nomad™, Boundary™, and Waypoint™. HashiCorp offers free community source-available products, enterprise products, and managed cloud services. The company is headquartered in San Francisco, though most HashiCorp employees work remotely, strategically distributed around the globe.
For more information visit hashicorp.com

www.hashicorp.com