HashiCorp | paloalto NETWORKS

Securing the Cloud Operating Model

Achieving the fastest path to value with a zero trust security model in a modern, multi-cloud world

Whitepaper

Contents

Executive summary

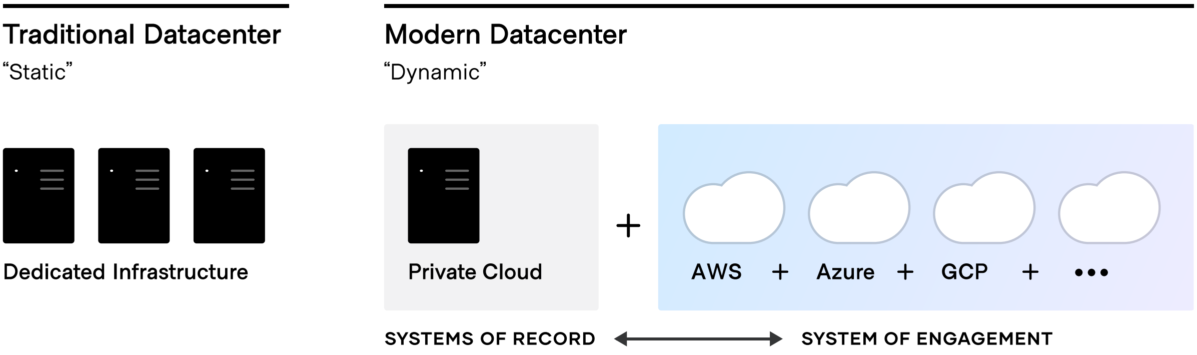
For most enterprises, digital transformation means delivering new business and customer value, more quickly, and at scale. The implication for enterprise IT is a shift from cost optimization to speed optimization. The cloud is an essential part of this shift, as it presents the opportunity to rapidly deploy on-demand services with limitless scale.

Modern applications interact with the most important asset of every enterprise: customer data. As such, systems and applications need an aggressive, cloud-first security posture. Modern enterprises employ a comprehensive cloud security framework, one that is embedded into software development practices and automated at runtime. HashiCorp and Palo Alto Networks enable enterprises to easily access and gain the significant benefits of a secure cloud operating model with their closely integrated suite of security solutions.

This whitepaper details how HashiCorp and Palo Alto Networks empower organizations to successfully adopt a secure cloud operating model, with security scans and sensors strategically weaved into the application lifecycle and across diverse infrastructure targets.

Transitioning to a multi-cloud environment

The transition from traditional datacenters to multi-cloud environments is a generational shift for IT. This transition means shifting from largely dedicated servers in private environments to a pool of shared compute services available on-demand. While most enterprises began with one cloud service provider, there are good reasons to use cloud services from others. Each cloud provider is investing hundreds of millions of dollars on unique capabilities. Further, mergers and acquisitions can result in a multi-cloud strategy. The most successful organizations empower their teams to use the right cloud services for the job, resulting in multi-cloud adoption.

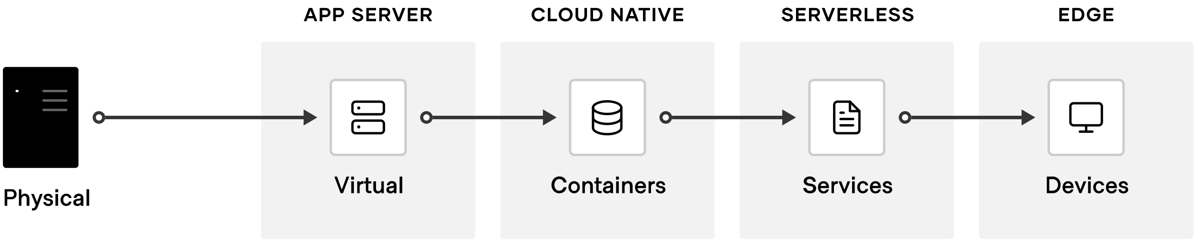


A secure cloud operating model presents an opportunity for increasing operational speed and scale, optimized for new "systems of engagement" — applications built to engage with the customer and user. These new critical apps are the primary interface for customers to engage with a business and are aligned to benefit from cloud delivery. These new greenfield apps:

- Have dynamic usage characteristics, and must scale up and down under variable traffic
- Must support rapid iteration, and quickly add capabilities that improve the user experience

For most enterprises, these systems of engagement must co-exist with "systems of record" that are the core databases and internal applications which often run on-premises. As a result, enterprises end up with a complex hybrid environment - a mix of multiple public and private clouds.

There are two challenges that enterprises must overcome to achieve the many benefits of the cloud operating model. The first challenge is to determine how applications can be delivered in the cloud with seamless, reliable consistency. The second challenge is ensuring security is embedded throughout the software development lifecycle. The cloud operating model does not trade off innovation for comprehensive security, but in fact prioritizes both objectives. After all, both attributes are required.



For cloud computing to support innovation effectively, there needs to be a consistent workflow that scales securely and on demand across different cloud service providers (CSPs). In order to achieve this, the following is required:

- Consistent instruction sets for provisioning
- Identity for security and for network connections
- Privileges and rights so they can be deployed and run

Implications of the cloud operating model

The transition to the cloud operating model is a shift from "static" infrastructure to "dynamic" infrastructure. In a dynamic environment, practitioners focus on configuration, management, and automation - specifically provisioning, securing, connecting, and running cloud resources on demand.

	Static		Dynamic
Run	Dedicated infrastructure	→	Scheduled across the fleet
Connect	Host-based, Static IP	→	Service-based, Dynamic IP
Secure	High trust, IP-based	→	Low trust, Identity-based
Provision	Dedicated servers, Homogeneous	→	Capacity on demand, Hetergeneous

Decomposing this shift, and working up the stack, various changes of approach are implied:

- **Provision.** The infrastructure layer transitions from running dedicated servers at limited scale to a dynamic environment where organizations can easily accommodate increased demand by spinning up thousands of servers and scaling them down when not in use. As architectures and services become more distributed, the sheer volume of compute nodes increases significantly.
- **Secure.** The security layer transitions from a fundamentally "high-trust" world enforced by a strong perimeter and firewall to a "low-trust" environment without a clear or static perimeter. As a result, the foundational assumption for security shifts from being IP-based to using identity-based access to resources and adjusting to a zero-trust authentication and authorization model. This shift is highly disruptive to traditional security models.
- **Connect.** The networking layer transitions from being heavily dependent on the physical location and IP address of services and applications to using a dynamic registry of services for discovery, segmentation, and composition. Enterprise IT does not have the same control over the network, or the physical locations of compute resources, and must think about service-based connectivity.
- **Run.** The runtime layer shifts from deploying artifacts to a static application server to deploying applications with a scheduler atop a pool of infrastructure that is provisioned on-demand. In addition, new applications have become collections of services that are dynamically provisioned, and packaged in multiple ways, from virtual machines to containers.

	Static		Dynamic			
	DEDICATED		PRIVATE CLOUD	AWS	AZURE	GCP
Run Deployment	vSphere	→	vSphere	EKS / ECS Lambda	AKS / ACS Azure Functions	GKE Cloud Functions
Connect Networking	Hardware	→	Various Hardware	CloudMap AppMesh	Proprietary	Google Istio
Secure Security	IP: Hardware	→	Identity: AD/LDAP	Identity: AWS IAM	Identity: Azure AD	Identity: GCP IAM
Provision Operations	vCenter	→	Terraform	CloudFormation	Resource Manager	Cloud Deployment Manager

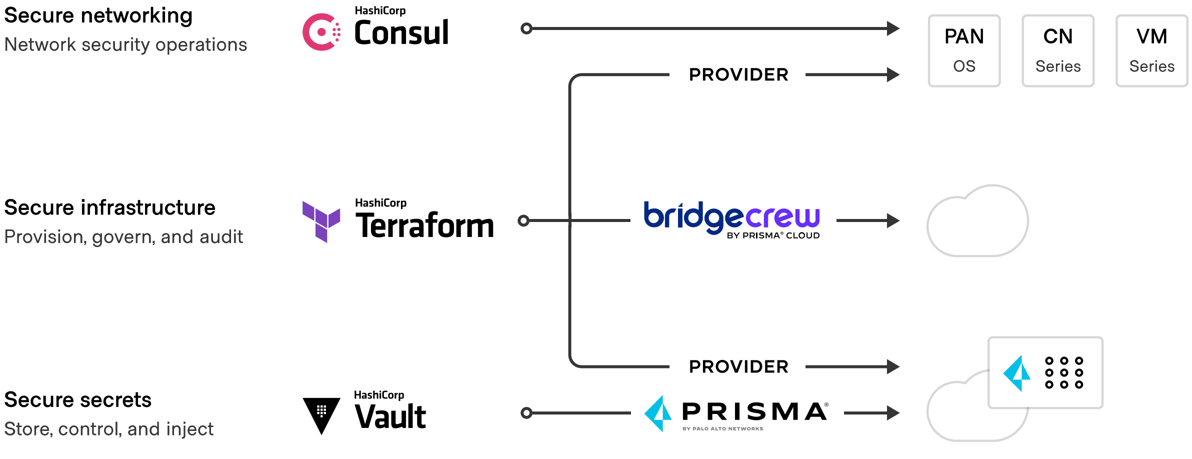
To address cloud operational challenges, teams should ask the following questions:

- **People**
    - How do we enable teams for a multi-cloud reality, and what skills can be applied with consistency across multiple environments?
    - How do we foster a collaborative environment for all stakeholders, especially among security, cloud, and DevOps teams?
- **Process**
    - How do we position central IT services as a self-service enabler of team speed and agility versus a ticket-based gatekeeper of control, and still retain strong compliance and governance?
    - How do we empower DevOps and cloud teams to take on greater security responsibility?
- **Tools**
    - How do we ensure adoption of comprehensive cloud-native tools that integrate security across the application lifecycle, technology stack, and into hybrid and multi-cloud environments?
    - How do we best capture CSP value to drive customer and business innovation?

Securing the cloud operating model with HashiCorp and Palo Alto Networks

The implications of the cloud operating model span infrastructure, security, networking, and applications. As such, enterprise IT is reorganizing around centers of excellence (CoE) and centralized shared services. This popular model simplifies the delivery of the dynamic infrastructure and services necessary for modern development teams.

As CoE teams deliver each shared service in the cloud operating model, the velocity of innovation increases. In fact, the greater an organization's cloud maturity, the faster its pace of innovation. Central to this velocity increase: security considerations "shift left" to earlier in the application lifecycle.



IT leaders should keep three major milestones in mind as they adopt the cloud operating model.

1. **Establish the cloud essentials.** Enterprises beginning their cloud journey should address a few immediate requirements. Practitioners often seek to adopt infrastructure as code, establish compliance and governance guardrails, and ensure regular security monitoring. These fundamental building blocks enable teams to accelerate the adoption and deployment of dynamic cloud architectures.

   This initial milestone also requires cloud-native security practices. Specifically:

   a. **The effective use of modern tools.** Ensure IT and cloud teams can rapidly deliver business value at greater scale with modern CI/CD, security, and DevOps tooling.

b. **The adoption of compliant cloud operations.** Ensure integrations offer comprehensive compliance enforcement across build, deploy, and run phases (DevSecOps) to secure the cloud operating model.

c. **Embrace autoscaling.** Establish automatic scaling rules to ensure application uptime and resiliency.

d. **Establish and acknowledge a shared security model.** Reinforce partnerships with trusted security solutions like Vault and Prisma Cloud that have demonstrated success across industries and across major CSPs.

2. **Standardize on a set of shared services.** Enterprises gain efficiencies by standardizing on a common set of shared services in a cloud operating model. The portfolio of shared services should balance developer choice and flexibility with a realistic maintenance burden for operations teams.

   Similarly, enterprises need to take steps to secure interactions with shared services. Specifically:

   a. **Cloud Security Posture Management (CSPM).** Ensure workload and data visibility, guardrail compliance, and governance, including least privilege recommendations, all within simple interfaces that span clouds.

   b. **Cloud Workload Protection (CWP).** Ensure host, container, web application, API and serverless operations are monitored and defended for threats and risk in operations, including at runtime.

   c. **Cloud Network Security (CNS).** Enforce identity-based microsegmentation to prevent lateral movement of threats and achieve a zero-trust architecture.

   d. **Cloud Infrastructure Entitlement Management (CIEM).** Ensure IAM permission enforcement across workloads and clouds.

3. **Innovate using a common logical architecture.** As teams fully embrace the cloud and depend on elastic services and modern applications as the primary systems of engagement, there will be a need to create a common logical architecture. This requires a control plane that connects with an extended ecosystem of popular solutions. Enterprises can also perform advanced cloud security management and orchestration across multiple services and clouds.

   To effectively reach this third milestone in the cloud operating model, enterprises must ensure uniform and comprehensive security management and orchestration across multiple and hybrid cloud environments and at every layer. Specifically:

a. **Deep security integration leveraging a unified framework.** Ensure defense-in-depth protection with a uniform platform able to deliver layered security for all workloads within a single pane of glass and with a single agent.

b. **Integrated cloud-automated vulnerability and threat intelligence. E**nsure integrated operational threat intelligence from trusted upstream commercial, open source and proprietary data sources to ensure out-of-the-box protection for OWASP Top 10 application and zero-day threats.

c. **Uniform security across multiple clouds and hybrid environments.** Ensure seamless and secure communication across adjacent third-party services such as Slack, JIRA, and ServiceNow. This ensures employees remain productive and InfoSec teams gain visibility into distributed cloud security.

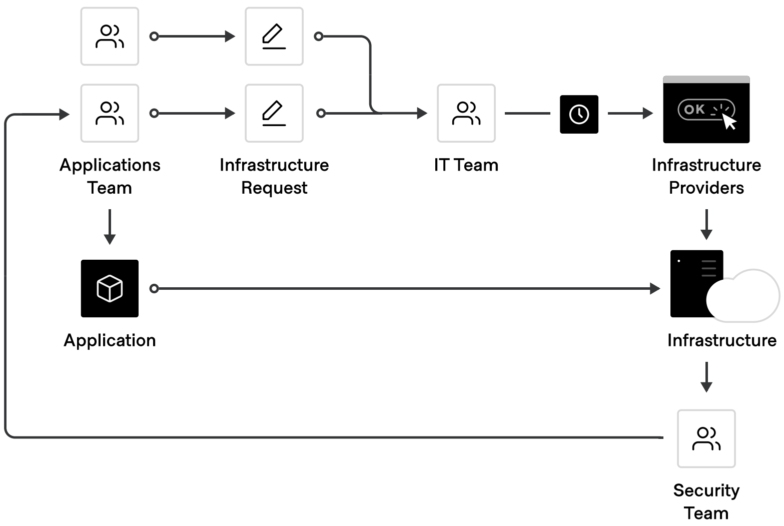
What follows is a review of how to successfully adopt a secured cloud operating model with HashiCorp and Palo Alto Networks.

Enhancing Security at the Infrastructure Layer (“Provision”)

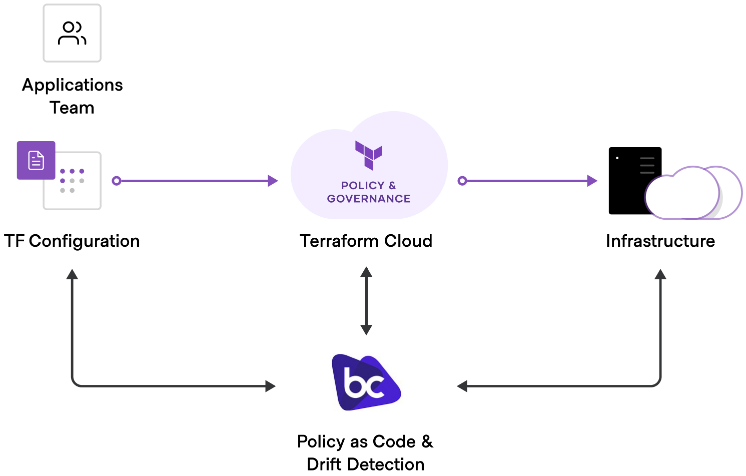
The foundation for adopting the cloud is automated infrastructure provisioning. HashiCorp Terraform is the most widely used cloud provisioning product. Terraform can be used to provision infrastructure for any application using an array of providers for any target platform. With Terraform, DevOps teams can represent and deploy complex infrastructures at scale and across a multi-cloud environment. However, it is equally important to ensure that the components of the infrastructure definitions in Terraform are appropriately secured to prevent attacks, exploits, and breaches. This can be achieved by adopting purpose-built tools from Bridgecrew by Prisma Cloud to scan the Terraform configurations as they are built, in order to detect security errors arising from misconfigurations or high-risk configurations.

To achieve shared services for infrastructure provisioning, IT and cloud teams should start by implementing reproducible infrastructure as code practices, and then layering security, compliance, and governance workflows to ensure appropriate controls.

Before Terraform & Bridgecrew by Prisma Cloud



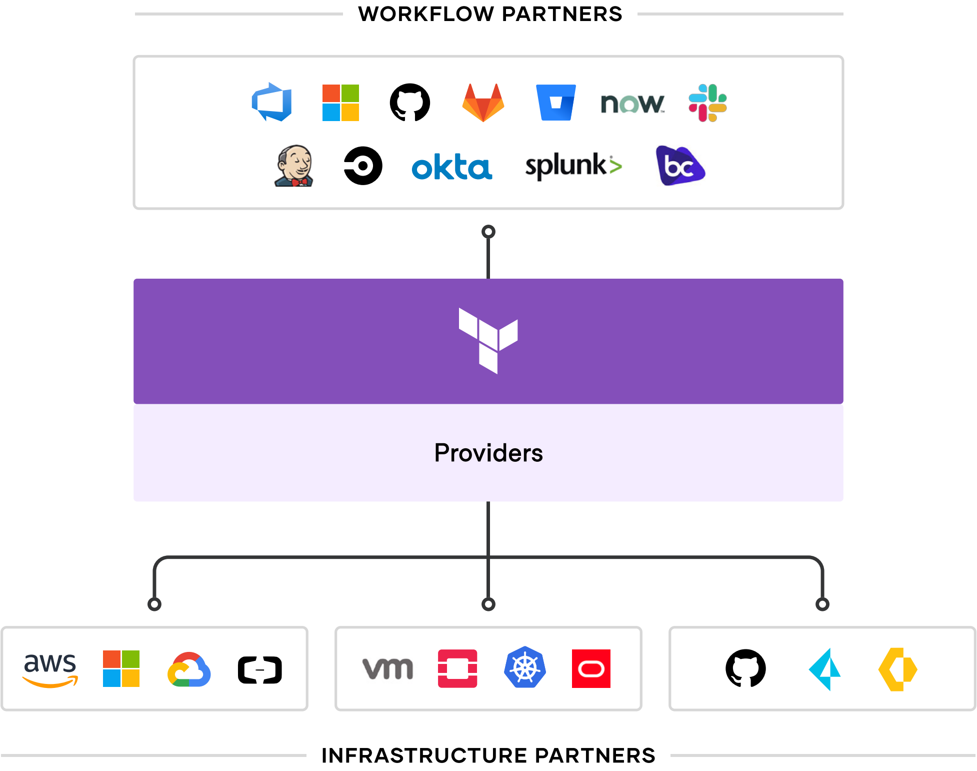
After Terraform & Bridgecrew by Prisma Cloud



Reproducible Infrastructure as Code

The first goal of a shared service for infrastructure provisioning is to enable the delivery of reproducible infrastructure as code, providing DevOps teams a way to plan and provision resources inside CI/CD workflows using familiar tools throughout.

DevOps teams can create templates in the form of Terraform modules. Modules express the configuration of services from one or more cloud platforms in a simplified manner. Terraform integrates with all major configuration management tools to allow fine-grained provisioning to be handled following the provisioning of the underlying resources. Finally, modules can be extended with services from many other ISV providers to include monitoring agents, application performance monitoring (APM) systems, security tooling, DNS, and content delivery networks, and more. Once defined, these reusable templates can be provisioned as required in an automated way. In doing so, Terraform becomes the lingua franca and common workflow for teams provisioning resources across public and private clouds.



For self-service cloud and IT, the decoupling of the template-creation process and the provisioning process greatly reduces the time taken for any application to go live, since as long as they use a pre-approved template, developers no longer need to wait for operations approval.

Shift Security Left with Secured Infrastructure as Code

Security in the cloud is a shared responsibility. Specifically, security of the cloud is the responsibility of the cloud provider, while security in the cloud is the customers' responsibility. CSPs constantly strengthen their security capabilities, and have a reliable track record of rapid innovation. Consequently, ensuring that the infrastructure that is deployed and the services consumed are strongly secured is the responsibility of the security, cloud, and DevOps teams within an enterprise.

However, it is a challenge for teams to stay abreast of all the best-practice security requirements, guidelines, and configurations. The Bridgecrew by Prisma Cloud "infrastructure as code" scanning tools can be leveraged to scan IaC configurations and modules for security policy violations and misconfigurations at various stages in the development pipeline: in the IDE, in the pull-request phase, within the CI/CD pipeline, through to runtime. Sentinel, HashiCorp's policy as code framework, can also be used to embed logic-based policy decisions directly into the Terraform workflow itself. The advantage of this approach is that DevOps teams receive immediate and contextual security telemetry - and in languages developers understand - with remediation guidance delivered early in the development phase to significantly improve posture, reducing out-of-cycle feedback. Enterprises benefit from feedback that integrates seamlessly into the agile methodologies of DevOps teams to compliment speed and agility with security.

Extending Zero-Trust Security ("Secure")

Dynamic cloud infrastructure means a shift from host-based identities to application-based identity, over low-trust networks across multiple clouds without a clear network perimeter.

In the traditional security world, internal networks were assumed to have high trust, so anything within the four walls was assumed secure. This is often referred to as the castle-and-moat approach to security: fortify the walls and control entry and exit through a single door. With a modern "zero-trust" approach, the assumption is that no IP address or endpoint on the network can be trusted and every access request must be verified. This requires that applications and access be explicitly authenticated and authorized to fetch secrets and perform sensitive operations, all of which are tightly audited.

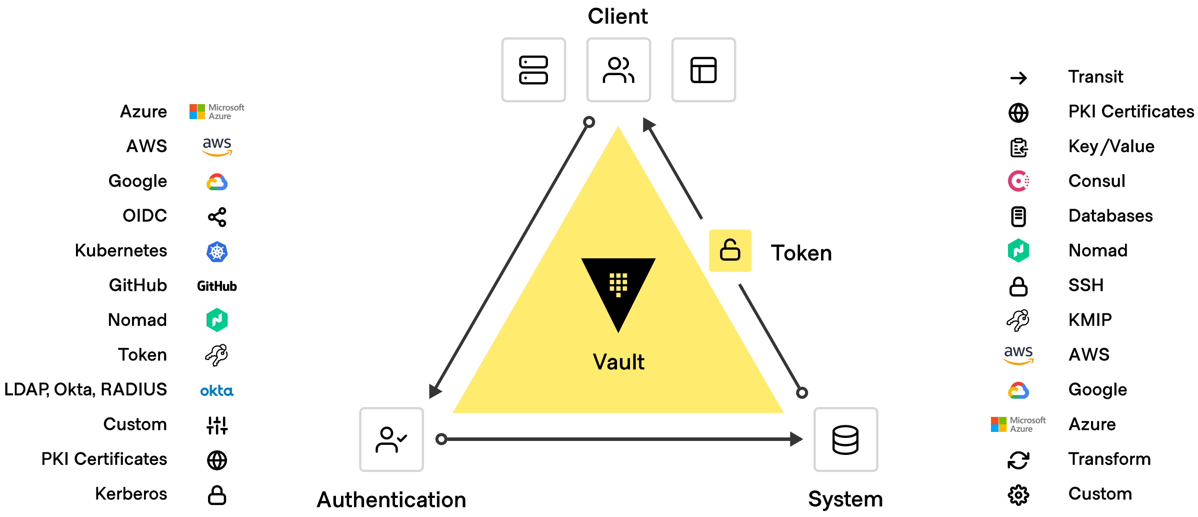
Secrets Management

HashiCorp Vault enables teams to securely store and tightly control access to tokens, passwords, certificates, and encryption keys for protecting machines and applications. This provides a comprehensive, best-in-class secrets management solution. Additionally, Vault helps protect data at rest and data in transit. Vault exposes a high-level API for developers to secure sensitive data. Vault also can act like a certificate authority to provide dynamic, short-lived certificates to secure communications with SSL/TLS. Lastly, Vault enables a brokering of identity between different platforms, such as Active Directory on premises, or AWS IAM to allow applications to work across platform boundaries.

Vault is widely used across some of the largest organizations, including stock exchanges, financial organizations, retail, manufacturing, and governments, to provide security in the cloud operating model at scale across different verticals and use cases.

To achieve shared services for security, IT teams should enable centralized secrets management services, and then use that service to deliver more sophisticated use cases such as certificate and key rotations, and encryption of data in transit and at rest.

Prisma Cloud integrates with Hashicorp Vault in order to facilitate the seamless, just-in-time injection of secrets for cloud and containerized applications. Consequently, developers need only specify a reference to the secrets in the Kubernetes YAML file. Prisma Cloud in turn intercepts the deployment of the container, retrieves the secrets from Vault, and injects them into the container.



Enterprise IT and cloud teams should build a shared service that enables the request of secrets for any system through a consistent, audited, and secured workflow.

Encryption as a Service and Advanced Data Protection

Additionally, enterprises need to encrypt application data at rest and in transit. Vault can provide encryption as a service with a consistent API for key management and cryptography. This allows developers to perform cryptographic operations through a single API and then protect data across multiple environments. Using Vault as a basis for encryption as a service solves difficult problems faced by security teams, such as certificate and key rotation.

While many enterprises provide a mandate for developers to encrypt data, they do not often provide the "how," which leaves developers to build custom solutions without an adequate understanding of cryptography. Vault provides developers a simple API that can be easily used, while giving central security teams the policy controls and lifecycle management APIs they need.

As enterprises leverage the cloud for critical applications, there has been a simultaneous growth in the storage of sensitive customer data in cloud storage services such as Amazon S3, Azure Blob Storage, and others. Prisma Cloud provides visibility, classification, and governance capabilities to ensure that data stored in cloud-persistence storage are appropriately secured to prevent data exfiltration.

Enterprises with high security requirements for data compliance (PCI DSS, HIPAA, and more) have additional challenges. Advanced data protection provides the functionality for data tokenization, such as data masking, to protect sensitive data such as credit cards, sensitive personal information, bank numbers and more. This capability protects data and cryptographically protects anonymity for personally identifiable information (PII).

Visibility, Compliance, and Governance

Enterprise security practice needs to start with full visibility and assessment of the compliance posture of cloud assets. HashiCorp Sentinel enables the definition of deployment policies in order to establish guardrails to enforce governance on cloud deployments. Prisma Cloud provides out-of-the-box compliance to assess, monitor, and alert on the security posture of assets deployed in cloud environments using comprehensive industry best-practice and compliance standards. Prisma Cloud also enables security teams to "shift left" and adopt DevSecOps with purpose-built security tools that integrate into developer IDEs and across the CI/CD pipeline to detect violations prior to deployment. These visibility, compliance, and governance capabilities are extended even further with integrated Machine Learning (ML) based algorithms that raise cloud configuration and network data flow alerts. Prisma Cloud has also implemented two Terraform providers to help teams automate onboarding and configuring a large number of cloud accounts onto the platform, deploying and managing a large fleet of Defenders or adding and managing users accounts in the platform.

Securing Workloads

Enterprises are leveraging heterogeneous cloud stacks by incorporating workloads that run on VMs, containers, and serverless platforms. These workloads are characterized by scale and high ephemerality, and are treated as immutable infrastructure. Prisma Cloud provides cloud-native protections by moving security closer to the workloads, defining policies based on cloud metadata such as labels and tags, and autoscaling to match the workload lifecycle. Enterprises can leverage Prisma Cloud in order to meet security and compliance outcomes such as:

- **Vulnerability assessment** for hosts, containers, applications, and serverless
- **Runtime protection** embedded into workloads with machine learning for automated real-time response that only allows sanctioned process, file system, and network activity within the runtime
- **Policy definition and governance** using cloud and container tags and labels to deliver a flexible policy framework that scales automatically
- **Intelligence integration** with trusted industry threat feeds to inform and protect against zero-day threats

The combination of Sentinel to enforce enterprise wide deployment policies and Bridgecrew by Prisma Cloud to provide hundreds of out-of-the-box policies for cloud providers and Kubernetes provides enterprises the ability to establish cloud security guardrails while not inhibiting operational or DevOps agility. Centralized teams codify policies to enforce security, compliance, and operational best practices across all cloud provisioning. The automated enforcement of policies ensures changes are compliant without creating manual review bottlenecks. Further, drift detection can identify when manual changes are made to cloud workloads so that cloud infrastructure and Terraform templates can be brought back in sync in accordance with GitOps best practices.

IAM Governance

IAM permissions determine the actions that a user or role can perform in the cloud. A number of cloud breaches are the direct result of adversaries exploiting overly permissive IAM roles. However enterprise security and cloud teams have struggled to identify, remediate and rectify user roles with excessive permissions. The Prisma Cloud platform enables security teams to address these security concerns by monitoring excessive and unused permissions, through ML-powered UEBA, and with least privilege recommendations and remediation capabilities.

Enhancing Security at the Networking Layer ("Connect")

The challenges of networking in the cloud are often some of the most difficult aspects of adopting the cloud operating model for enterprises. The combination of dynamic IP addresses, a significant growth in traffic originating within the network (known as east-west traffic) as the microservices pattern is adopted, and the lack of a clear network perimeter pose a formidable challenge. Additionally, the dynamic nature of cloud workloads adds to the complexity of securing the network.

Networking services should be provided centrally, where IT and cloud teams provide service registry and service-discovery capabilities. Having a common registry provides a "map" of what services are running, where they are, and their current health status. The registry can be queried programmatically to enable service discovery or drive network automation of API gateways, load balancers, firewalls, and other critical middleware components.

HashiCorp Consul provides a multi-cloud service networking layer to discover and securely connect services. Consul can also dynamically program the Palo Alto Networks VM-Series firewall with security policies in order to protect the workload and application.

Service Discovery

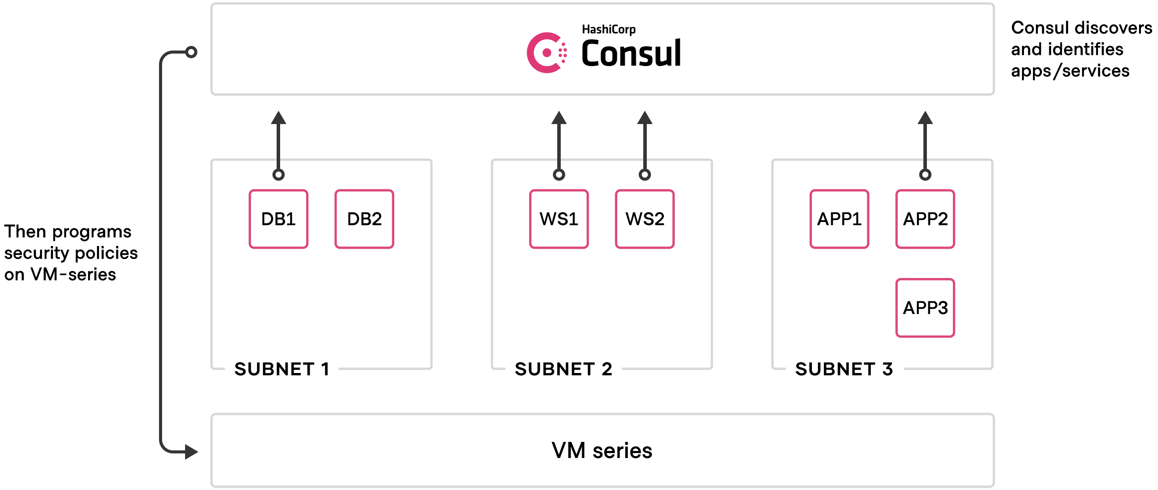
The starting point for networking in the cloud operating model is typically creating a common service registry, which is used as a real-time directory of what services are running, where they are, and their current health status. Traditional approaches to networking rely on load balancers and virtual IPs to provide a naming abstraction to represent a service with a static IP. For Consul, each service is programmatically registered and DNS and API interfaces are provided to enable any service to be discovered by other services. Consul also provides integrated health checks in order to track and monitor application availability. Consul can also be integrated with traditional load balancers and container orchestration platforms such as Kubernetes.

Consul can be integrated with other services that manage existing north-south traffic - such as traditional load balancers and distributed application platforms such as Kubernetes and Nomad-to provide a consistent registry and discovery service across multiple -environments, clouds, and platforms.

Network Infrastructure and Security Automation

The next step is to reduce operational complexity with existing networking infrastructure through automation. Instead of relying on a manual or ticket-based process to reconfigure load balancers and firewalls every time there is a change in service network locations or configurations, a process that can take days or weeks, Consul can be used to automate these network operations without operator intervention.

The integration between the Palo Alto Networks VM-Series firewall and HashiCorp Consul demonstrates the ability to seamlessly discover new application or service deployments and the configuration of security policies to provide in-depth protection from attacks. For example, when a DevOps team deploys a new service in the cloud, HashiCorp Consul automatically discovers various properties of the application and uses these properties to program dynamic address groups on the VM-Series firewall. These dynamic address goups are in turn associated with security policies which are then automatically applied to protect these new applications from network-based attacks. The integration between a service discovery platform such as Consul and a next-generation firewall such as the VM-Series enables DevOps and network security teams to meet the security needs for highly elastic and dynamic application deployments.


HashiCorp Consul
Consul discovers and identifies apps/services
Then programs security policies on VM-series
DB1
DB2
SUBNET 1
WS1
WS2
SUBNET 2
APP1
APP2
APP3
SUBNET 3
VM series

Securing the Network

Security teams need to extend the “zero-trust” posture and to secure cloud workloads from a network perspective. This includes protection from network access originating from outside the enterprise network, commonly referred to as “north-south” traffic, as well as traffic originating from workloads within the network, the aforementioned “east-west” traffic.

The Palo Alto Networks VM-Series virtual firewalls provide best-in-class, next-generation firewall capabilities to protect cloud networks from malicious attacks. The VM-Series delivers inline network security that inspects communications for applications, users, content, and threats as well as blocks any malicious attempts over the network. These capabilities allow security teams to deploy fine-grained security policies to permit access based on application and user identifiers and other transport-layer attributes, while all other network access is denied. Additionally, the VM-Series protects workloads from never-before-seen malware and zero-day attacks using inline machine learning and the Wildfire service in order to identify and block malware.

Automation of this deployment and configuration is critical for agility and success in the cloud. Palo Alto Networks has fully automated the deployment of best-practice architectures to the VM-Series to secure all cloud environments using simple infrastructure as code templates such as Terraform, CFTs, ARM templates, and others. The Palo Alto Networks Terraform provider further enables security teams to represent all aspects of their configuration and security policy as structured code. These capabilities provide security teams with unprecedented agility to meet the security needs of highly dynamic cloud applications and environments.

Prisma Cloud Identity-Based Microsegmentation then secures inter-service communication - commonly known as east-west traffic - by employing fine-grained policies based on the identity of the applications. Prisma Cloud assigns every host and container a cryptographically signed workload identity. Security and DevOps teams define network and security policies based on identities that are then enforced by each workload. As workloads intercommunicate, Prisma Cloud uses identity to authenticate and authorize requests before granting network access to the application. Only workloads verified by their identity are allowed to communicate on the network.

Enhancing Security at the Runtime Layer ("Run")

Modern applications come in many diverse formats, such as containerized microservices and VM-based applications. Cloud-native runtime security supports the entire stack and the customer responsibility as a part of the cloud shared-responsibility model, from infrastructure configurations to application code. Addressing each piece separately or in silos only recreates the challenges of on-premises security where uncorrelated alerts create too much noise and fatigue for security teams.

Effective runtime security requires a defense-in-depth approach to adequately secure running applications in the cloud. It begins with secure cloud infrastructure. Above that, securing the network, as addressed in the previous section, protects entrance into and all lateral movement among services. Securing the orchestrator that schedules services creates a safe platform for vetted containers and VMs to run on.

Secure Orchestration

Nomad by default provides a secure orchestration layer for containerized and legacy workloads to provide confidentiality, integrity, and authentication. Nomad deployments can further enhance security with the addition of mTLS, ACLs, and namespaces to segment workloads and provide deep access control. Sentinel policies provide granular control to enforce governance over Nomad orchestration, such as task drivers.

Prisma Cloud secures CI/CD environments and provides Nomad with vetted images. The Prisma Cloud solution identifies vulnerabilities and misconfigurations in container images and, offers remediation guidance - Nomad pulls those secured images for safe deployment into the runtime.

Full-Stack Cloud Security

Prisma Cloud delivers full-stack runtime security for containerized and VM-based cloud workloads. Cloud infrastructure including configurations, networking, and IAM layers are secured. Securing scaled cloud workloads requires continuous vulnerability management and compliance monitoring, enhanced with machine learning and modeling that automates governance and control so that malicious or anomalous actions cannot be taken by a container or host. Prisma Cloud provides cloud-native security at all of these layers, as outlined in the previous sections.

Conclusion: securing the future

Unlocking the fastest path to value in multi-cloud and hybrid environments is achieved by adopting a secured, common cloud operating model. Business leaders can embrace modernity across enterprise IT and cloud teams in three key areas:

1. **People: Shifting to multi-cloud skills**
   - Reuse incumbent skills and consistently extend expertise and best practices to multi-cloud and hybrid environments.
   - Embrace comprehensive security "shifted left" with DevSecOps and other agile practices to deliver elastic, resilient, distributed systems.
2. **Process: Shifting to native self-service**
   - Position IT and cloud teams as an enabling shared service focused on application delivery velocity and embedded security, allowing them to ship software faster with less risk.
   - Establish centers of excellence with correlated, built-in guidance across each layer of the cloud for self-service delivery of security and governance.
3. **Tools: Shifting to dynamic environments**
   - Use tools - including full lifecycle security - that support the increasing ephemerality and distribution of infrastructure, applications, containers, and serverless runtimes. Optimize support for critical workflows rather than specific technologies.
   - Provide policy and governance tooling to match the speed of delivery with compliance to manage risk in a self-service environment.

A cloud-native security posture often requires a combination of solutions. To this end, HashiCorp and Palo Alto Networks have partnered to help leading enterprises reduce risk and adopt zero-trust security principles.

The companies work alongside enterprises to protect customer data and critical systems with shared services and solutions across each layer of the modern IT stack. Together, we help you provision, secure, connect, and run any infrastructure for any application.

HashiCorp

www.hashicorp.com