SOLVED OVERVIEW

The joint VMware and Caveonix Cloud solution offers a fully integrated security, compliance, and governance platform to effectively manage data sovereignty compliance requirements of hybrid multi-cloud environments.

The Caveonix Cloud platform has been fully tested and validated to support the VMware Cloud Foundation (VCF) components including, VCloud Director (VCD), vCenter, vSphere, VMware Tanzu Kubernetes Grid (TKG), vRealize Automation (vRA), NSX-V and NSX-T.

The platform assesses the security posture of the VMware environment and provides continuous monitoring to ensure immediate reporting and mitigation of any drift in the security and compliance posture, thus protecting all data assets stored in the VMware sovereign cloud.

This multi-tenant platform when integrated with VCF enables service provider partners to provide a secure and compliant infrastructure and platform services for customers via their cloud offerings. The service providers can support deployments in their data centers as well as extend the capability to customer data centers as external cloud deployments.

Caveonix’s ability to provide security and compliance monitoring comes from object-level checks on best practice requirements recommended by VMware to create and deploy secure compliance zones in their service provider infrastructure. This is fully automated from deployment within the service provider environment and integrated through VMware’s Cloud Software Defined Data Center (SDDC) and Software Defined Network (SDN) technology stack in a compliant manner within the VMware Sovereign cloud boundary.
Caveonix Cloud continuously detects, predicts, and acts to mitigate cloud risk, ensuring a continuum of security, compliance, and governance risk management for the hybrid cloud.

JOINT USE CASES

Create Secure Data Center Infrastructure Environment for VMware Sovereign Cloud
Setup infrastructure that meets the compliance and governance requirements for sovereign cloud within the service provider’s data centers as well as customer data centers on managed services basis.

Provide Compliance Zones Within Sovereign Cloud Environment
Provide customers with compliant cloud infrastructure that meets state, national and global regulatory compliance requirements such as GDPR, BSI C5, PCI, and HIPAA, creating differentiated service offerings in the market.

Enable Continuous Compliance Monitoring
Monitor changes in highly dynamic cloud environments for drift in security and compliance posture across on-prem and external data centers. Caveonix Cloud provides automated testing of compliance controls as well as the ability to document manual controls using the built-in governance, risk, and compliance (GRC) module.

Unified Sovereign Cloud Reporting
Service Providers and their customers can manage and report on the security and the compliance posture as well as the overall risk in their applications deployed in the sovereign cloud, from a single integrated dashboard. Caveonix's integration with VMware SDDC stack and the external cloud provides unified visibility of the security, compliance, and governance postures across 38+ regulations. This unified dashboard prevents blind spots and any digital risk involved with sovereign cloud implementation and customer data protection.
Monitor Security for data-at-rest and data-in-transit

a. Caveonix cloud performs assessments of the infrastructure as well as the platform services, to ensure that the data at rest is protected using encryption and is using the right encryption algorithms across various OS and data storage solutions in the sovereign cloud boundary. Based on 10,000+ security and compliance policy checks, Caveonix assesses whether the workloads are running applications securely in virtual machines or containerized environments.

b. Caveonix integrates with VMware Cloud Foundation components and captures network flows plus the associated metadata via its Application Programming Interface (API) integration with NSX-T. This creates a visual flow map of communication to identify application inter-dependencies. The flow-specific metadata is also used to validate that the communication is encrypted and employs the right crypto libraries for protecting data in transit.

DEPLOYMENT ARCHITECTURE

The Caveonix Cloud architecture is flexible, enabling VMware Cloud Provider partners with localized deployment of the platform as an application within the VMware Sovereign cloud boundary. The platform monitors and enforces segmentation based on compliance zones and regulatory boundaries from infrastructure to platform to application. All stakeholders (service providers, customers) have full access to this information in the local environment of the VMware sovereign cloud boundary.

The Caveonix Cloud dashboard implements very strong attribute-based access control (ABAC) and role-based access control (RBAC), allowing only authorized personnel to access information, maintain access control and take action related to any privacy data/information stored in the sovereign cloud boundary. This information is locked for audit controls and reporting requirements. Also, the infrastructure application-specific security checks and remediation steps are fully documentable, based on automated testing of technical controls and full documentation of non-technical controls through the Caveonix Cloud Governance Risk and Compliance (GRC) module to support all the audit and compliance artifacts for demonstrating compliance with data sovereignty requirements.
BETTER TOGETHER

BENEFITS OF CAVEONIX CLOUD PLATFORM FOR VMWARE SOVEREIGN CLOUDS

**UNIFIED 360° VISIBILITY ACROSS ALL VMWARE CLOUD ASSETS**

Clear visibility of all data and applications assets on-premises and on-cloud.

**A SINGLE INTEGRATED PLATFORM THAT UNIFIES SECURITY, GOVERNANCE, AND COMPLIANCE**

Unified enterprise dashboard for managing hybrid cloud IT risk, at scale.

**SUPPORTS OVER 38+ REGULATIONS**


**GREATER CONTROL OVER INFRASTRUCTURE COMPLIANCE ACROSS ALL VMWARE INFRASTRUCTURE COMPONENTS**

Integrates effectively with VCloud Director (VCD), vCenter, vSphere, VMware Tanzu Kubernetes Grid (TKG), vRealize Automation (vRA), NSX-V and NSX-T.

**ENABLES DELIVERY OF MANAGED SECURITY AND COMPLIANCE SERVICES**

Generate new revenue by managing hybrid multi-cloud environments and compliance on behalf of customers while also gaining internal efficiencies within their environment due to increased automation and reporting ease of use.

**INTEGRATES WITH CLOUD-NATIVE MICRO-SEGMENTATION FUNCTIONS**

Whitelisting and blacklisting network policies using VMware NSX-T.