Thales CipherTrust Manager and VMware Cloud Director Encryption Management Solution

Better Securing Sovereign Cloud Workloads

Outstanding benefits of the industry-leading Thales CipherTrust Manager

- A centralized platform for key and policy management across on-premises data repositories and cloud infrastructures.
- Simplifies key lifecycle management tasks Including secure key generation, backup/restore, clustering, deactivation, and deletion.
- Streamlines administrative tasks through a self-service licensing portal.

The demand for operational independence from cloud service providers has surged in today's digital landscape. This quest for autonomy encompasses pivotal aspects, such as managing encryption keys—an indispensable facet, particularly in scenarios where data sovereignty assumes paramount importance. In highly regulated sectors and government entities, the focal point is the establishment of zero-trust environments designed to provide undisputable authority upon them, enabling the explicit ownership and governance of their most sensitive data assets.

In response to this increasing demand, VMware has entered a strategic partnership with the Thales Group, a renowned leader in cybersecurity solutions and a trailblazing innovator in enterprise key management. This collaboration leverages VMware Cloud Director's capabilities in conjunction with Thales CipherTrust Manager's cutting-edge expertise. Together, this solution equips businesses with a centralized approach for managing encryption keys, fine-grained access control, and the flexibility to customize security policies to align precisely with their requirements.

Thales CipherTrust Manager proven interoperability with VMware Cloud Director Encryption Management solution

CipherTrust Manager and the newly introduced VMWare Cloud Director Encryption Management pave the way for Sovereign tenants to use their encryption keys (BYOK) or even their entire key management system (BYOKMS) during the virtual machine creation and encryption process. While providers can anchor this Sovereign service within their Sovereign Cloud infrastructure, they must remain blind to key access — a privilege solely reserved for the customers. The foundational premise is straightforward: providers maintain zero visibility into the encryption keys, ensuring they remain strictly within Sovereign borders.

Customer outcomes of using Bring-Your-Own-Encryption-as-a-Service with VMware Cloud Director Encryption Management, which addresses several critical security and control considerations:

- Data Security
- Compliance Requirements
- Data Ownership
- Customized Encryption Policies
- Key Rotation and Access Control
- Transparent Monitoring and Auditing
- Risk Mitigation
- Scalability
- Multi-Cloud Support and
- Efficient Disaster Recovery

Built upon innovative cloud technologies, CipherTrust Manager represents a cloud-attuned key management solution. Its REST interface, paired with a microservice-based architecture, delivers simplified deployment and inherent scalability. The value of CipherTrust Manager lies in its ability to manage keys and policies centrally and to simplify complex key lifecycle management tasks. From secure key generation, backup, and restoration to clustering, deactivation, and deletion, CipherTrust Manager provides a centralized hub for managing encryption keys across disparate encryption appliances.

Bring-Your-Own-Encryption as a Service with VMware Cloud Director Encryption Management

VMware Cloud Director is a leading cloud management platform designed to facilitate the deployment, management, and orchestration of true multi-tenant cloud infrastructure, allowing service providers and enterprises to deliver and manage cloud services efficiently.

The VMware Cloud Director Encryption Management solution with Bring Your Own Encryption as a Service (BYOEaaS) functionality offers several advantages for organizations seeking to enhance their data security, compliance, and control in a cloud environment. This approach allows customers to manage encryption keys while leveraging the services provided by VMware Cloud Director.

The security offering adheres to full Sovereign compliance, enabling Sovereign tenants to utilize their encryption keys (BYOK) and/or their key management system (BYOKMS) to create and encrypt virtual machines in VMware Cloud Director. Providers can host this Sovereign service within their Sovereign Cloud infrastructure, but they cannot access the keys. Only customers will possess the keys, and providers will have no visibility. Providers will guarantee that encryption keys remain confined within the Sovereign boundaries.

In summary, the VMware Cloud Director with Encryption Management solution add-on and Thales CipherTrust Manager offer a comprehensive solution for organizations looking to enhance data security, meet compliance requirements, and maintain control over their encryption practices. This combination enables businesses to enjoy the benefits of cloud services while maintaining data protection and control.

Use Cases of this Solution

Tenants bringing their own Key (BYOK):

In the context of Sovereign Cloud, the concept of 'Tenants Bringing Their Own Encryption Keys' (BYOK) has gained growing prominence and importance. BYOK involves organizations, typically those operating as cloud tenants, being able to exercise control and authority over the encryption keys used to secure their data. This practice offers a multitude of advantages, making it a key strategy for bolstering data security in today's digital landscape.

One of the primary benefits of BYOK is its direct alignment with compliance requirements and regulations. Many industries and regions have strict mandates in place regarding data protection and encryption standards. BYOK allows organizations to ensure that their encryption practices adhere to these specific guidelines, helping them avoid costly fines and legal repercussions. It assures that sensitive data is being protected in a manner that meets regulatory standards.

Moreover, BYOK empowers organizations with more control over their data. They can dictate how their encryption keys are generated, stored, and managed, enhancing their overall governance of sensitive information. This control is particularly valuable in data access and sharing cases, as organizations can grant or revoke access by managing the associated encryption keys.

In the current climate, marked by the ever-increasing frequency of data breaches and privacy concerns, BYOK serves as a strategic approach to fortify data security. Allowing organizations to take charge of their encryption keys ensures that even in the event of a breach, the compromised data remains unreadable to unauthorized parties. This additional layer of security acts as a formidable defense against cyber threats and breaches, reducing the risks associated with data exposure.

Furthermore, BYOK is especially valuable in the context of cloud and multi-cloud environments. As organizations increasingly rely on these platforms for data storage and processing, they can maintain consistent encryption practices across different cloud providers, ensuring data security regardless of the cloud infrastructure being utilized.

In summary, VMware Cloud Director Encryption Management solution represents a powerful tool for organizations seeking to safeguard sensitive information in an environment fraught with data security challenges. With its BYOK implementation, it ensures compliance with regulations and provides a level of control and protection that is vital in today's world of escalating data breaches and privacy concerns. BYOK offers a strategic means of embracing the advantages of cloud and multi-cloud environments while maintaining the highest data security and privacy standards.

Tenants bringing their own Key Management Server (BYOKMS):

The emerging trend of tenants adopting their own Key Management Servers (KMS) for data encryption represents a significant shift in the data security and control landscape. This practice empowers organizations with a level of customization

and control over their data encryption methods that was previously unattainable. It addresses several critical needs in the current data security landscape.

First and foremost, this approach allows organizations to tailor their encryption methods to their specific needs. By managing their KMS, they can implement encryption algorithms and standards that best suit their data protection requirements. This adaptability is particularly valuable in sectors with unique data security demands, such as healthcare, finance, and government, where sensitive data must be safeguarded with precision.

Furthermore, owning and managing a KMS enables organizations to meet regulatory requirements effectively. Many industries and regions have stringent data protection and encryption standards in place. By controlling their KMS, organizations can ensure that their encryption practices align with these specific regulations. This compliance helps organizations avoid costly fines and builds trust with customers and partners who demand robust data security measures.

This approach is especially advantageous for organizations operating in multi-cloud or hybrid cloud environments. These complex setups demand precise, compliant data security solutions that adapt to various cloud infrastructures and configurations. Owning and managing a KMS allows organizations to maintain consistent data security across diverse cloud providers, ensuring that their sensitive data remains well-protected regardless of the cloud environment being utilized.

In conclusion, the trend of tenants adopting their own Key Management Servers for data encryption signifies a significant advancement in data security and control. It empowers organizations to customize encryption methods, meet regulatory requirements, reduce vendor lock-in risks, and, most importantly, strengthen data security in an era marred by data breaches and privacy concerns. This strategic approach is advantageous for organizations seeking precise, compliant data security solutions in multi-cloud or hybrid-cloud environments.

Targeted for Regulated Enterprises and VMware Sovereign Cloud Providers

This solution is the result of a thorough and meticulous approach, tailored to the precise needs of regulated enterprises and providers that operate within the VMware Sovereign Cloud ecosystem. Its design and functionality are carefully honed to cater to the specific challenges and compliance requirements that are intrinsic to these organizations.

In today's dynamic business environment, there is an increasing emphasis on safeguarding data, ensuring its sovereignty, and ensuring strict compliance with an array of regulations. For businesses operating in sectors like healthcare, finance, and government, and many others, these concerns are particularly acute. The stakes are high, with sensitive data, confidential information, and the trust of clients and citizens on the line.

This solution is the answer to these pressing needs. It comes equipped with a comprehensive set of tools and capabilities, meticulously developed to not only address the unique requirements of these industries but also to excel within them. It's a proactive approach that doesn't just meet the demands of regulations but also goes a step further to enhance data protection, privacy, and regulatory adherence.

This solution becomes a critical asset for enterprises and cloud providers navigating the complexities of highly regulated and sensitive environments. It empowers them to operate with confidence, knowing that they have the technology and support to comply with the stringent rules and standards governing their operations. In essence, this solution is more than a software package; it's a strategic advantage, providing the means to not only meet regulatory requirements but to excel in highly regulated and sensitive sectors.

Operating via VMware Cloud Foundation on the VMware Sovereign Cloud Ecosystem

In the current landscape, there is a growing awareness of the importance of data sovereignty and a notable increase in the stringency of regulatory requirements. To navigate this complex terrain, the implementation of a Sovereign Cloud Ecosystem on the **VMware Cloud Foundation** offers organizations a powerful solution to create a cloud infrastructure that not only complies with these regulations but is also highly secure and tailored to specific geographic regions and industry requirements.

At the heart of this approach is VMware Cloud Foundation (VCF), a comprehensive and robust platform known for its ability to manage cloud environments efficiently. It streamlines the deployment and operation of cloud infrastructure, offering an integrated, automated, and standardized environment that simplifies the management of virtualized data centers. VCF's capabilities include compute, storage, networking, and cloud management services, which enable organizations to optimize their cloud resources, enhance agility, and improve overall operational efficiency.

These represent several business models that can be accommodated within a standardized architectural framework, illustrating how VMware Cloud Foundation is employed for the deployment and management of VMware Cloud Director tenancies for both our enterprise and the cloud provider.

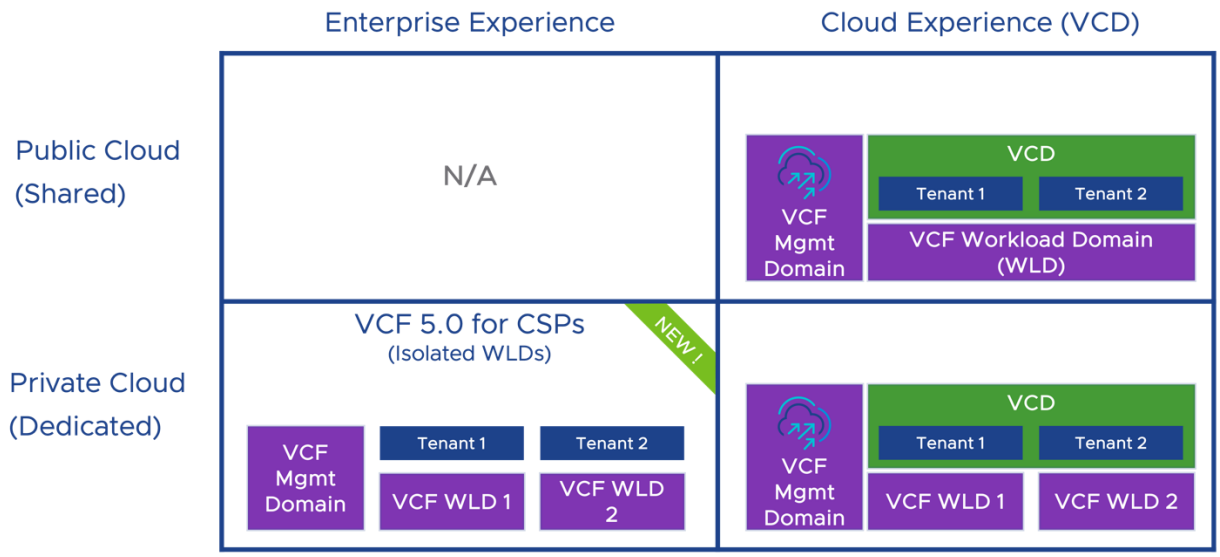

Figure1: Delivering Simplification with Integrated Stacks (VCF + VCD)

Complementing this robust foundation is the Sovereign Cloud Ecosystem, a carefully crafted portfolio that's purpose-built to address the unique needs of specific regions and industries. This specialized stack provides organizations with the tools and configurations necessary to ensure data sovereignty and regulatory compliance while meeting the specific demands of local jurisdictions and industry regulations.

With the Bring Your Own Key (BYOK) and Bring Your Own Key Management System (BYOKMS) capabilities the VMware Cloud Director Encryption Management emerges as a critical solution in bolstering the security posture of VMware Cloud Director (VCD) and VMware Cloud Foundation (VCF) within sovereign cloud environments. By allowing organizations to retain control over their encryption keys, BYOK empowers them with a higher level of data protection and compliance adherence. This means that even within the confines of a sovereign cloud, where stringent data sovereignty regulations prevail, organizations can ensure that their sensitive information remains safeguarded. With VMware Cloud Director Encryption Management, VCD and VCF users can confidently store, transmit, and process data, knowing that they have full control over the keys that safeguard it, fortifying their position in compliance audits and bolstering their overall security stance in the sovereign cloud landscape. This capability not only facilitates regulatory adherence but also provides a greater sense of ownership and trust in the security of cloud-based operations.

In essence, the combination of VMware Cloud Foundation and the Sovereign Cloud Ecosystem empowers organizations to establish cloud infrastructures that meet the rigorous demands of today's data privacy regulations and provide the security and flexibility required to thrive in specific geographic and industry contexts. This approach helps organizations navigate the complexities of data sovereignty and regulatory compliance confidently while reaping the benefits of a dynamic and efficient cloud infrastructure.