Provider Scenario:

Sovereign Cloud

Scenario overview

Specific country regulations and compliance rules require data to not leave a sovereign area. Many countries have stringent regulations and compliance rules that require data not to leave a sovereign area. Yet many of the large hyperscalers are outside these areas. These regulations highlight many data privacy risks and the growing need to protect national, corporate, and personal data. It’s possible that data residing in a cloud inside or outside of a sovereign area can be collected and queried by a government agency if it is within their legal jurisdiction. Increased attention for protecting personal privacy information on how government authorities collect and use data about individuals across the globe is becoming more of a threat. To prevent unwanted exposures or compliance violations, the data must reside in a sovereign area.

Customers in industries or governments are looking for a solution that provides enforcement of data and workload residency, extends data sovereignty protections beyond the immediate platform where possible and enables secure, audited connectivity and data transaction between resident, sovereign, and non-sovereign data classifications.

Key differentiators

Ransomware protection
• Secure Restore from Veeam® ensures that if undetected malware is included in backups, the restore process can leverage a wide range of antivirus or anti-malware tools to scan for the malicious components with actual detection of patterns at the time of restore.
• Anomalistic data activity monitors if a backup size increases substantially, most likely due to encryption by malware. Veeam ONE™ monitoring captures this in real time on production VMs by scanning vCenter and sees the attack before it creates the backup.
• While running in a VMware Sovereign Cloud data center, Veeam’s ransomware protection enables cloud customers to be ready for ransomware attacks, recover with confidence and overcome any cyberthreat.
• Solution provides comprehensive ransomware remediation with automated backup verifications and fast, reliable recovery.
Leverage immutable object storage in separated sovereign area against ransomware
• Veeam works with several S3-compatible Object Storage providers like Cloudian in highly scalable sovereign data centers.
• Cloudian HyperStore and Veeam Availability Suite™ support compliance mode Object Lock for air-tight data immutability all the way up to the operating system root level to protect data from ransomware attacks.
• Backup data copies are tamperproof for a set period of time, which prevents hacker encryption or deletion while ensuring a clean data copy for reliable recovery.

Sovereign security and compliance requirements
• Veeam data protection supports each sovereign security domain for resident backup and sovereign backup isolated from one another and is aligned with VMware’s NSX-T rigorous isolation and firewall sovereign requirements.
• Veeam supports multi-tiered storage options, hybrid cloud and multi-cloud within sovereign policies and data can be stored based on long-term retention policies for sovereign regulatory or compliance needs.
• Combined solution of VMware, Cloudian and Veeam enables customers to enforce their policies for data staying within a resident or sovereign zone.

Hurt

Broad questions — How do they do it today?
• How do you assure data never leaks out of a specified region?
• Is cyber recovery becoming a concern as part of business continuity plans?

Credibility questions
• How much would your fines be if data left a sovereign area?
• How much would you be willing to pay after a ransomware attack?

Plausible emergency

How would you feel if…?
Your customers data leaked out of a region or was interrogated by an out of region government? Or, if the fines violating geo specific compliance rules impacted your customer’s profitability? Or their business came to a grinding halt as their data was encrypted by ransomware?
What if instead...?
Your confidence increased by ensuring all data never leaves a region, backups are immutable and therefore protected from a direct ransomware or hacker attack with fast recovery. The 3-2-1-1-0 processes are including immutable backup storage for ransomware protection and your risk is lowered for non-compliance while preventing your business from being held hostage by bad actors.

Rescue

Usage scenario
• A comprehensive package with VMware's Sovereign SDDC reference architecture based on vCloud Foundation or optional vCloud Director, Intrinsic Security based on NSX, Compliance with vRealize Suite, Veeam Availability Suite and Cloudian HyperStore provide an out of the box fully integrated solution.
• Veeam with the appropriate antivirus ransomware detection/remediation can help lower your TCO for cyber insurance, lower the probability of ransom payments which have no guarantees and allow you to avoid legal & moral hazards.

© 2022 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.