VMware Sovereign Cloud Initiative with Veeam & Cloudian

Immutable backups to help you fight ransomware attacks, recover with confidence and overcome any cyberthreat.

VMware Sovereign Cloud framework provides both guiding principles and best practices for delivering cloud services that can meet security, compliance and data sovereignty requirements of a specific cloud operating jurisdiction as mandated by the relevant government or commercial body. Data that is classified to reside in a Sovereign area should not leave that area through the use of appropriately segregated VMware-intrinsic networking firewalls and security policies with backups protected by Veeam with Cloudian Immutable Storage.

VMware Sovereign Cloud

Sovereign Clouds help protect and unlock the value of critical data (e.g., national data, corporate data, and personal data) for both private and public sector organizations. This helps improve control of data, demonstrates compliance with privacy laws, and delivers a national capability for digital innovation. Sovereign clouds are about more than data sovereignty. While the location of data and jurisdictional control of data is important, sovereignty clouds must provide customers with the confidence they need to deploy critical apps and data. Customers want assurances that all their sensitive data is properly managed, secured and controlled by a trusted cloud provider.

A sovereign cloud must have five characteristics to provide the assurances customers need:
- Data sovereignty and jurisdiction control
- Data access and integrity with secure protection
- Data security and compliance
- Data independence and mobility
- Data innovation and analytics

While adherence to stringent regulations can ensure that no data leaks out of a sovereign region, it doesn’t address bad actor attacks against the data resident in a sovereign area. Thus, it’s vital to ensure that this mission-critical data can be defended against these attacks, be protected and enable a rapid recovery in the event of a malicious attack.

Figure 1: Sovereign Cloud Characteristics
What is ransomware?

Ransomware is malicious software that infects a computer and restricts access to crucial user data until a ransom is paid to unlock it. Ransomware is designed to spread through your network, exploiting technical and human vulnerabilities and leading to a significant impact on your business. Ransomware has dramatic consequences. Cybersecurity Ventures\(^1\) predicted that cybercrime would cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015. The average recovery cost per attack is now $84,000. In its 2021 Ransomware Study\(^2\), IDC also stated that the average ransomware payment was $240,000 and that over a third of respondents reported that ransomware caused a business disruption of at least one week.

At Veeam\(^*\), we believe secure and immutable backup is your last line of defense against ransomware. Our software will help you by design with immutable backups. It can be the difference between downtime, data loss and paying a costly ransom. While running in a sovereign cloud data center, Veeam can provide:

- Comprehensive ransomware remediation
- Infrastructure flexibility
- Automated backup verifications
- Fast, reliable recovery

With Veeam’s ransomware protection as part of the Veeam Availability Suite\(^*\), VMware Sovereign Cloud customers can be ready for ransomware attacks, recover with confidence and overcome any cyberthreat.

Cloudian HyperStore object storage complements Veeam Availability Suite with a fast, disk-based hybrid-cloud storage and built-in data immutability for ransomware protection. At 70% less cost than traditional enterprise storage\(^3\), Cloudian offers an innovative solution for better backup storage.

Comprehensive ransomware remediation solution

To remediate ransomware threats, organizations must implement a combination of people, processes and tools that perform a series of functions; identify, protect, detect, respond and recover.

Completing only one of these functions is not enough to fight ransomware. Thus, organizations need a comprehensive backup solution to perform all functions.

With Veeam and Cloudian, a broad set of capabilities is provided that help organizations fulfill the 5 functions of ransomware remediation for their backup solution.

1. Identify; Veeam ONE\(^*\) which includes workload grouping by Business View
2. Protect; Backup immutability, air-gap backup options, access security with encryption for data at rest and in-motion.
3. Detect; Backup Integrity verification with Malware scanning, Veeam ONE Ransomware detection
4. Respond; Veeam Virtual Lab, SureBackup\(^*\)
5. Recover; Secure Restore, Instant Recovery

VMware Sovereign Clouds security domains

All VMware Sovereign Clouds must include two prescribed security domains. First, the resident domain represents an area with the highest degree of trust and confidence where all member elements reside within the geographical boundary of the jurisdiction. No data should be stored or processed outside of the jurisdiction and no network traffic ever traverses hardware that is not assured to be within the local geography. No element of the domain can be deemed to be under the control or influence of foreign or non-sovereign entities. The resident domain only accepts traffic from systems in its parent sovereign domain and other qualified resident domains within the same country or pan-national entity, it has no route to and from the public internet or other provider networks.

Second, the sovereign domain represents an area of reduced trust and higher risk mitigation in which network connectivity between member systems and non-sovereign systems is possible on an exceptional basis. This domain serves use cases in which the customer application cannot be entirely isolated and is required to interact with external and on-premises systems. Storage and processing within the sovereign domain would primarily still be resident in the local geography, however, the sovereign domain does allow for the possibility of replication or data transfer outside of the jurisdiction but with enhanced protections such as encryption at-rest and in-flight.

\(^1\) https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
\(^2\) https://www.idc.com/getdoc.jsp?containerId=US48093721
\(^3\) https://cloudian.com/tco/
Cloudian and Veeam in a VMware Sovereign Cloud

Ransomware became a top priority for CIOs, as it is now omnipresent. The costs of ransomware go beyond the ransom, including damage or loss of data, downtime, lost productivity, post-attack disruption to the normal course of business, forensic investigation and reputational harm.

Data immutability has become a must-have feature to obtain cyber insurance and maintain business continuity. Sovereign data needs to be protected against attacks with immutable storage providing similar to air gap the functionality that a hacker cannot delete, encrypt or manipulate the backup data. Since multiple copies of the immutable storage need to be kept on at least two different places, a cost-effective backup target solution is key. Veeam is integrated with Cloudian Object Storage to achieve this goal.

- To protect data from ransomware attacks, Cloudian HyperStore and Veeam Availability Suite support Object Lock for air-tight data immutability all the way up to the storage operating system root level.
- This permits backup data copies to be made tamperproof for a set period of time, which prevents hacker encryption or deletion and ensures a clean data copy for reliable recovery. The resulting security is comparable to offline storage.
- Both Veeam and Cloudian support multi-tenancy, ensuring that multiple clients may be supported within a single sovereign cloud while maintaining stringent access, and data security as well as separation. Integrated billing simplifies management, and QoS controls help you deliver consistent service levels.

Moreover, increasingly sophisticated ransomware attacks that specifically target backup data and administrator functions make it critical for organizations to ensure that their backup platform has ransomware remediation capabilities.
Veeam Availability Suite with Cloudian HyperStore together provide a platform to protect and manage all workloads, enabling your business to evolve as you manage data while ensuring its availability across any application or cloud infrastructure. Together with VMware Sovereign Cloud, it can enable critical sovereign data workloads and provide the ultimate defense and protection for them.

**Figure 4: Veeam with Cloudian Object Lock**

- **Secure Software Design Data Center**
  - VMware Cloud Foundation with the addition of Cloud Director delivers accelerated Cloud infrastructure with ecosystem support and security at its core.

- **Better data visibility & protection**
  - Understand where data exists and which users need to access it through microsegmentation.

- **Enable network security controls**
  - Quickly identify and adjust privileges for certain data types through microsegmentation dynamic firewall policies.

- **Staged and secure data restore**
  - Ensure recovered virtual machines don’t contain any personal or sensitive data to meet compliance standards.

- **Ransomware workload testing**
  - Restore data in an isolated virtual sandbox, scan for malware, without impacting production systems.

- **Immutability backups**
  - Secure options on premises and in the cloud using Veeam Scale-out Backup Repository™ (SoBR) & Cloudian HyperStore.

- **Item-level recovery**
  - Perform item-level recovery from application-aware backups with Veeam Explorers™ for Microsoft applications.

- **Instant VM Recovery and database (DB) recovery**
  - Restore VMs and DBs to your production environment by running them from compressed and deduplicated backup files.

- **Storage flexibility**
  - Over 163 qualified or integrated storage options, including over 32 object storages, of which 19 are immutable, makes the 3-2-1-1-0 rule easy.

- **Intrinsic Security**
  - NSX provide end-to-end security consistently across the solution & supports enforcement of data sovereignty and residency boundaries.

- **Compliant Service Design**
  - vRealize Operations monitors and provides capacity analytics for compliance management along with ongoing capacity, resource utilization monitoring, and alerting to prevent outages and service degradation.

- **Real-time data protection monitoring and alerts**
  - Maintain visibility and mitigate issues with 340+ pre-set alarms and 150+ pre-built reports and Heatmaps.

- **Workload discovery**
  - Automatically discover new workloads and applications to determine the best process for a successful backup.

- **Confident recovery orchestration**
  - Dynamically update and automate the testing of recovery plans and quickly recover any data without manual intervention.

**Figure 5: VMware, Veeam & Cloudian capabilities for sovereign cloud**