Business challenge

Many countries have stringent regulations and compliance rules that require data to not leave a sovereign area. Yet many of the large hyperscalers are outside these areas, limiting how mission-critical workloads can move to public clouds. 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.

Increased attention for protecting personal privacy information on how government authorities collect and use data about individuals across the globe is surfacing to become more of a threat. To prevent unwanted exposures or compliance violations, the data must therefore reside in a sovereign area.

Customers in industry or government 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.

Solution overview: “Unified for You”

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 though. While the location of data and jurisdictional control of data is important, sovereign 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.

VMware Sovereign Cloud initiative is a framework that 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. VMware Sovereign Cloud provides the tools needed to enforce data privacy and security restrictions, auditability, assign classifications to data assets, offer comprehensive value-add services for industry and government, and a trusted platform for hosting both traditional and modern workloads flexibly and reliably.

Data that must reside in a sovereign area will not leave that area and is appropriately segregated out by VMware-intrinsic NSX edge and microsegmented networking firewalls and security policies with backups protected by Veeam®. Veeam greatly complements the initiative by completing the solution focused on backing up the data in the sovereign area, providing rapid SLAs in event of an attack or disaster.

Cloudian HyperStore forms the scalable and secure cloud storage layer. Built on de-facto cloud standards, with in-built multi-tenancy, billing, metering, QOS and industry leading security, Cloudian allows Sovereign cloud providers to enable offer equivalent services as the public cloud.

Now customers can be assured that their data will not leak out of a sovereign area while offering all the services that their customers require, and that the data is backed up in the sovereign area with the possibility to fast restore the workloads in a second sovereign cloud in the same geo jurisdiction in case of an emergency.
Figure 1: VMware Sovereign Cloud with Veeam Availability Suite & Cloudian HyperStore

Use Cases

Ransomware Defense & Protection

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 it’s 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 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 ransomware protection as part of Veeam Availability Suite™ with Cloudian HyperStore, VMware Sovereign Cloud customers can be ready for ransomware attacks, recover with confidence and overcome any cyberthreat. Veeam's Secure Restore ensures that if malware is activated in a backup, the backup can be restored to a previous state with the malware removed.


\(^2\) [https://www.idc.com/getdoc.jsp?containerId=US48093721](https://www.idc.com/getdoc.jsp?containerId=US48093721)
Rapid RPO/RTO
Mission-critical enterprises require fast recovery of their business in the event of an attack or disaster.
• Veeam's Continuous Data Protection (CDP) allows near zero RPO times while ensuring data consistency
• Solution allows direct recovery from HyperStore at the capacity tier without the need to rehydrate primary backup to achieve low Recovery Time Objectives (RTOs)
• Veeam CDP-based VM replication is included in Veeam's core license at no extra cost
• CDP also supports VMware vSphere encryption ensuring protection of sovereign data within the VMs

Leverage Immutable Object Storage in Sovereign area against Ransomware
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 that air gap capability and the ability to write data only once to ensure the integrity of the backup. Since multiple copies of the immutable storage are kept, Object Storage is the key repository target to provide the most cost-effective target. Veeam integrates seamlessly with S3-compatible Object Storage providers like Cloudian.
• 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 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

Recovery SLAs:
In the event of attack or disaster, it is critical that the required SLAs are met. It is also vital that proof of your disaster plan can be shown to any regulatory body in a sovereign area on demand, to meet the stringent sovereign compliance requirements.
• Veeam ONE™ complements VMware vRealize by aggregating backup availability and SLA metrics with monitoring that can flag potential issues before they occur
• Meet your compliance and regulatory auditor’s requirements with Veeam’s automated and detailed DR reports to create the DR plan definition, DR plan readiness, DR plan test while saving administrators considerable time while improving confidence with auditors
• Ensure you recover exactly what you need — no more, no less — with granular advanced search and find functionalities

Meet Sovereign security and compliance requirements:
As part of the overall VMware Sovereign Cloud intrinsic security value proposition, protecting the data in backups or off site is also a stringent sovereign requirement.
• Veeam supports each sovereign security domain aligned with NSX rigorous isolation and firewall requirements. This ensures industries or governments are enabled with at least two security domains for resident backup and sovereign backup isolated from one-another
• Veeam supports multi-tiered storage options, hybrid cloud and multi cloud within sovereign policies
• One can easily store data based on long-term retention polices for sovereign regulatory or compliance needs
• The combined solution of VMware and Veeam ensures data never leaks out of a resident or sovereign zone
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.

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

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

Stop lateral spread
of threats
Create micro-perimeters around specific sets of data and information.

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.

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.

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

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

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

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

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.

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

Benefits

• Ensures data remains in sovereign area, allowing it to be protected according to relevant regulatory bodies or country laws

• Creates a sovereign domain that represents an area of reduced trust with higher-risk mitigation in which network connectivity between member systems and non-sovereign systems is possible on an exception basis

• Protects backup files from ransomware in the event of a ransomware attack that would encrypt data and hold it hostage

• Allows full intrinsic security with networks and monitoring of VMware through data protection and monitoring with Veeam

• Offers any and all services with full security and data sovereignty with Cloudian HyperStore Cloud Storage

• Provides comprehensive ransomware remediation with backup into immutable storage from Cloudian, anomalous data activity monitoring and secure restore

Figure 2: VMware, Veeam & Cloudian capabilities for sovereign cloud
Conclusion

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. VMware, Veeam and Cloudian is the one platform to protect and manage all VMware workloads for data protection, enabling your business to evolve as you manage data while ensuring its availability across any application or cloud infrastructure. Together with VMware’s Sovereign Cloud initiative, it can provide the ultimate defense and protection for those critical sovereign data workloads.

Learn more

veeam.com