WHITE PAPER–OCTOBER 2020

Three Guidelines from Three Ministries - Japan

VMware Cloud on AWS

This whitepaper provides guidance on how VMware Cloud on AWS addresses the key requirements in Three Guidelines from Three Ministries (3G3M) published by the following three ministries in Japan:

- Ministry of Health, Labor and Welfare - Guideline for the Security Management of Medical Information Systems
- Ministry of Economy, Trade and Industry - Security Management Guideline for Information Processing Providers Dealing with Medical Information
- Ministry of Internal Affairs and Communication - Security Management Guideline for Cloud Service Providers Handling Medical Information

Executive Summary

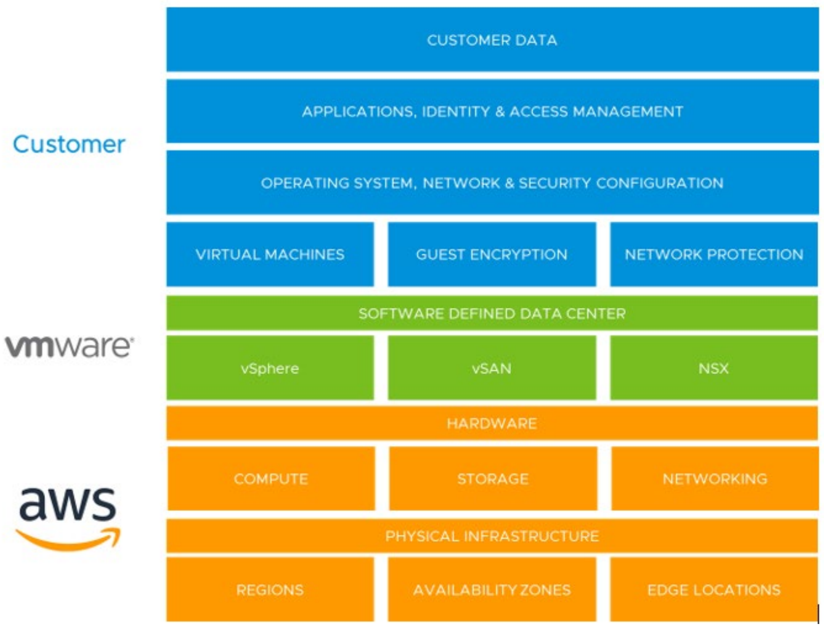
Digital innovation has transformed how healthcare organizations deliver patient care. While it has opened opportunities to improve the quality and delivery of patient care and reduce operational costs, it has created unique challenges in maintaining security and availability of healthcare information and systems, scaling up IT infrastructure with changing business demand and complying with stringent government mandates surrounding data security and privacy.

To enable healthcare organizations to manage patient and healthcare information in a secure and reliable way, the three Japanese ministries - Ministry of Health, Labor & Welfare, Ministry of Economy, Trade & Industry and Ministry of Internal Affairs & Communication have laid out guidelines for healthcare organizations and cloud service providers on various security measures to be followed when hosting patient and health care data externally. These are collectively known as Three Guidelines from Three Ministries (3G3M). This paper explores how VMware Cloud on AWS solution addresses the key requirements in these guidelines. To complement this whitepaper, VMware has also published security reference guides which describe how VMware Cloud on AWS helps meet many of these requirements in the three guidelines.

Shared Responsibility

Because customers (medical institutes/healthcare providers) retain control over their content, they retain responsibilities relating to that content as part of a “shared responsibility” model. This shared responsibility model is fundamental to understanding the respective roles of the customer and VMware and AWS.

This matrix of responsibility helps ensure higher overall security and helps eliminate single points of failure. The following diagram illustrates the high-level architecture for VMware Cloud on AWS and the associated security responsibilities for VMware, AWS and cloud tenants.



Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware responsibility "Security of the Cloud" – VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS.

AWS responsibility "Security of the Infrastructure" – AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the service

Communications Security

Securing data in transit is key when transferring data externally. VMware Cloud on AWS's defense in depth mechanism helps customers protect healthcare data in transit. There are two options for helping to secure data in transit to a customer's SDDC:

- **Over public internet:** For connectivity over the public internet between the customer's datacenter and the VMware Cloud on AWS Software Defined Data Center, customers may create IPsec VPN tunnels which support the most common encryption methods.
- **Via dedicated link:** VMware Cloud on AWS also provides customers with the ability to use the AWS Direct Connect service to establish a private virtual interface from the customer's on-premises network directly to the Software Defined Data Center, providing customers with a private, high bandwidth network connection. Customers may choose to establish an IPsec VPN within the AWS Direct Connect for creation of discrete virtual networks for dedicated purposes.

The cloud control plane supporting VMware Cloud on AWS is hosted on Amazon Web Services. (AWS) and is used to help protect from unauthorized network access by AWS Web Application Firewall, AWS monitoring services. Additionally, AWS logs are continually monitored by VMware's SIEM tool and any unusual activity is investigated by the VMware Security Operations Center.

Finally, all connectivity from the cloud control plane to the SDDCs used for management and monitoring is protected with industry standard encryption mechanisms.

Electronic Storage Requirements

Maintaining security, preservability, and readability of healthcare data is a pivotal for healthcare organizations. VMware Cloud on AWS provides multiple layers of encryption to help ensure the security and integrity of the healthcare data on the cloud service.

- **Self-encrypting drives:** The i3.metal instances used by VMware Cloud on AWS contain eight local self- encrypting NVME drives. The Self-Encrypting Drives (SED) use AWS 256- bit XTS encryption and the keys for these drives are securely generated by the firmware on the drive itself. The use of self-encrypting drives helps protect customers from an individual with physical access to the datacenter being able to physically remove drives and access the contents of the drives.
- **VMware vSAN:** In addition to the data protection provide by the SEDs, VMware Cloud on AWS SDDCs utilizes VMware vSAN to protect customer content across a cluster. VMware vSAN is a software-defined storage (SDS) product developed by VMware that pools together direct-attached storage devices across a VMware vSphere cluster to create a distributed, shared data store. VMware Cloud on AWS has enabled de-duplication, compression and encryption by default for all clusters. These are settings are defined when a cluster is provisioned and cannot be turned on or off for individual clusters.

- **VMware vSAN encryption and key management:** VMware has integrated VMware vSAN with the AWS Key Management Service, (KMS) to provide a highly secure, highly available and cost-effective method of generating encryption keys to support vSAN encryption in all VMware Cloud on AWS regions. vSAN Encryption on VMware Cloud on AWS uses the AWS KMS service to generate a primary key, referred to as Customer Master Key (CMK). One CMK is generated per cluster and the CMK never leaves the HSM backed AWS KMS. The CMK keys cannot be accessed directly by either AWS or VMware employees.

Healthcare organizations in need of an additional level of encryption or who need to use their own keys or Key Management Infrastructure have the option to use third party encryption or security software within the guest operating system running on VMware Cloud on AWS. This offers flexibility and choice and enables medical institutes and health care providers to use the same security software they use in their own datacenters in the cloud. The partner solutions can be found on our marketplace: *VMware Cloud Marketplace*

VMware also provides the following backup and restore services:

Management infrastructure including vCenter Server, NSX Manager, NSX Controller, and VMware NSX Edge

Customers are responsible for all data protection, backup/archive and restoration of all customer Content and configurations created by the customer in the SDDC, including Virtual Machines, Content Libraries, Datastores, and Port Groups.

Technical Safety Management Measures

Implementing appropriate logical security controls helps enable healthcare providers to ensure that patient data is accessible only be appropriate individuals and environment is safeguarded with protections for infrastructure, applications, and end-point devices.

VMware Cloud Services has logically separated networks that restrict the customer's access to their own private networks. The services' system and network environments are protected by a firewall or virtual firewall to help ensure business and customer security requirements, as well as to ensure protection and isolation of sensitive data. Firewalls act as critical components of the VMware network and information security architecture and are used to restrict and control network traffic and access to systems, data, and applications. VMware firewalls are operated in compliance with the Infrastructure Security policy in order to support the protection of VMware information systems.

VMware has in place well-defined operational security standards, practices, and other guidance with which all teams within VMware must comply. These include prevention through configuration management and testing, as well as vulnerability detection, assessment, management, and mitigation.

VMware assesses vulnerabilities across information systems and applications on a frequent basis and whenever new potential vulnerabilities are reported or detected, using a wide range of tools and techniques including but not limited to scan engines, port discovery, and service fingerprinting. Access to such tools is as tightly controlled and restricted as access to the systems and applications themselves. Vulnerability remediation requires pre-installation testing before a patch or fix is applied, a rollback plan for configuration changes, and follow-up testing to verify the patch or fix was successful, as well as removal of affected protocols or functionality in their entirety.

Physical Safety Management Measures

Maintaining appropriate physical safety measures is a common requirement across the three guidelines. The ministries require both healthcare organizations and cloud service providers to ensure that the equipment, media, and physical servers hosting healthcare data are adequately protected against damage. VMware Cloud on AWS leverages AWS and Amazon's strict approach to data center security. AWS limits physical data center access to approved employees and contractors who have a legitimate business need for such privileges. All individuals are required to present identification and to sign in.

Physical access is controlled both at the perimeter and at all building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff also utilizes multi-factor authentication mechanisms to access data center floors.

AWS handles all physical equipment lifecycle. AWS uses techniques described in industry-accepted standards to ensure that data is erased when resources leave the service. When a storage device has reached its end of life, and to help ensure that no residual data can be exposed, AWS follows the procedures detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization"). This includes degaussing and physically destroying all magnetic storage devices

For more information on AWS controls and data centers, visit:
https://cloudsecurityalliance.org/star/registry/amazon
https://aws.amazon.com/compliance/data-center/data-centers/
https://aws.amazon.com/compliance/data-center/controls/

Business Continuity and Disaster Recovery

Since medical treatment is performed all-round the year, unavailability of service or healthcare data can result in disruption of patient care. During, COVID-19 healthcare organizations have further increased delivering digital patient care services such as remote patient monitoring, online delivery of prescriptions, and video consultations. As such it is critical to help ensure that IT infrastructure is robust enough to withstand disasters and can recover promptly to minimize any disruption in patient care. VMware offers enterprise resilience programs that include business continuity and disaster recovery mechanisms.

Business Continuity

VMware has a defined Information Security Program that includes Business Continuity and Disaster Recovery strategies for data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises. This program implements appropriate security controls to protect its employees and assets against natural and manmade disasters. As a part of the program, an automated runbook system is engaged to ensure policies and procedures are reviewed and made available to appropriate individuals. Additionally, these policies and procedures include defined roles and responsibilities supported by regular workforce training.

VMware ensures that security mechanisms and redundancies are implemented to help protect equipment from utility service outages. The security mechanisms and redundancies are in turn reviewed through regular audits. VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify dependencies, critical products, and services. The real-time status of the VMware Cloud Services along with past incidents is publicly available at *https://status.vmware-services.io/*

Disaster Recovery

VMware Cloud Services has multiple disaster recovery mechanisms in place to recover from multiple concurrent failures. Redundancy and blast isolation are built into the architecture of the service to ensure high availability of the VMware Cloud Services, including regional independence and separation of console availability and customer service availability. VMware Cloud Services leverage the specific underlying AWS provider's infrastructure to enable customers to run workloads in multiple areas within a region as well as in multiple geographic regions.

VMware monitors the service's infrastructure and receives notifications directly from AWS in the event of a failure. VMware has developed processes with AWS to help ensure that that we have defined responses in place if an upstream event occurs.

The VMware business continuity plans and documentation are reviewed annually as part of the enterprise independent attestation process. The VMware Information Security Management System (ISMS) is based on the ISO 27001 framework. Business continuity and redundancy plans are reviewed by VMware third-party auditors who will perform reviews against industry standards.

Incident Logging and Management

Identifying, logging, and resolving incidents in a timely manner is necessary to restore services rapidly and avoid business disruptions. VMware has a dedicated Security teams (Architecture, Product, Cloud Service, Operations, Governance, Compliance) to manage security initiatives across the organization. In addition, the VMware Security Operations Center and Incident Management teams are responsible for monitoring and handling all information security incidents.

The VMware Security Incident Response Team (vSIRT) is responsible for developing incident handling procedures, for handling incident management across VMware. The vSIRT team is notified by the Security Operations Center of any potential incident and participates in any investigation. If VMware becomes aware of a security incident on VMware Cloud on AWS that leads to the unauthorized disclosure or access to personal information provided to VMware as a processor, we will notify customers promptly without undue delay and will provide information relating to a data breach as reasonably requested by our customers. VMware will use reasonable endeavors to assist customers in mitigating, where possible, the adverse effects of any personal data breach.

Unlike other cloud service providers, access to VMware Cloud on AWS environments by VMware is captured in the vSphere logs. Customers will see all actions taken by a VMware Admin are captured in the logs and fully visible in vRealize Log Intelligence Cloud (VMware Cloud on AWS log aggregation portal).

Audit logs and telemetry monitoring data only come from the infrastructure supporting the customer dedicated SDDC. VMware does not provide services that would require any customer to allow/authorize VMware employees to access their virtual machines, operating systems, file systems, or data. VMware has no ability to access, view, or log any data that originates from within the customer workload environments.

Third Party Risk Management

Maintaining appropriate third-party risk management procedures is necessary to ensure that any third parties or sub-contractors/sub-processors handling patient data are delivering service as per requirements and handle data securely. VMware has a comprehensive sourcing and vendor risk management process and program to select providers that meet VMware requirements which include security provisions. Supplier agreements are in place to help ensure providers are compliance with applicable laws, security, and privacy obligations. Customers are responsible for using our solution in compliance with relevant laws and regulations.

VMware has a formal process to document and track non-conformance as a part of our Information Security Management System (ISMS), which monitors supplier performance and escalates issues as necessary. To assure reasonable information security across information supply chains, VMware also conducts risk assessments at least annually to help ensure appropriate controls are in place to help reduce the risk related to the confidentiality, integrity, and availability of sensitive information.

VMware has made SLAs, Terms of Service, Data Processing Addendums, and Privacy notices publicly available. To review these documents, visit https://www.vmware.com/download/eula.html

Compliance

As a cloud provider, the VMware Cloud on AWS is aligned with internationally recognized standards as evidence of our commitment to information security at every level of the organization and that the security program is in accordance with industry leading best practices. Platform and application security standards are consistent with industry-accepted guidance and standards, such as, but not limited to, NIST, ISO, and CIS. VMware Cloud on AWS have established an Information Security Management System (ISMS) based on ISO 27001 standards and SOC2 to manage risks relating to confidentiality, integrity, and availability of information.

VMware regularly conducts internal and external audits that include results from security and compliance assessments. The program utilizes internal/external audits as a way to measure the effectiveness of the controls applied to reduce risks associated with safeguarding information and also to identify areas of improvement. Internal Audit reviews controls on an annual basis to identify nonconformities and opportunities for improvement. VMware has multiple teams dedicated to defining information security standards, processes, and technologies. Product security standards and operation security standards are continually evolving to keep up with industry best practices and to help ensure compliance with relevant regulatory requirements.

Conclusion

VMware has implemented a wide range of security controls to help ensure we deliver a secure and reliable environment for healthcare organizations to manage their IT infrastructure needs and manage patient data in line with leading industry standards including the Three Guidelines from Three Ministries. You can view existing compliance and certifications for VMware Cloud on AWS at *https://cloud.vmware.com/trust-center/compliance*

VMware Cloud on AWS provides healthcare organizations with an enterprise ready SDDC that provides easy migration, simplifies the movement of workloads and is supported by a shared responsibility model to maximize flexibility and control.

VMware Cloud on AWS helps reduce the complexity by having the same consistent architecture and operations on-premises and in the cloud by providing a hybrid cloud solution that can truly scale with business, take advantage of existing teams, skillsets, tools, and processes and let healthcare organizations focus on what's most important—patient health and care.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.