Solution Brief

Fourteen Cloud Security Principles

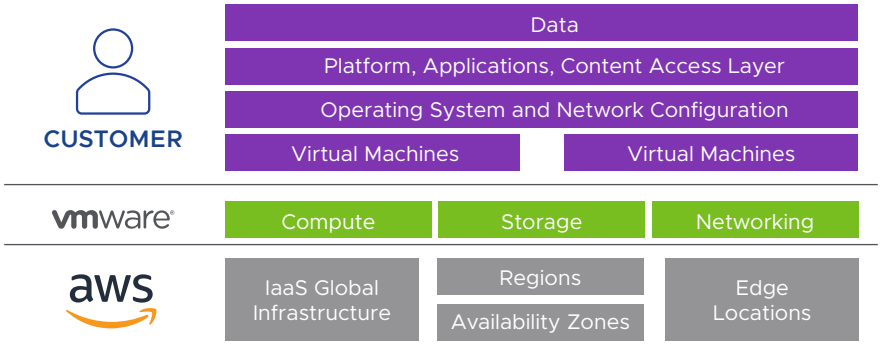
OVERVIEW

This whitepaper provides guidance on how VMware Cloud on AWS aligns with Cloud Security Principles and the objectives of these principles as part of NCSC Cloud Security Guidance.

Shared Responsibility

Because VMware customers 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, VMware and AWS in the context of Cloud Security Principles.

This matrix of responsibility ensures higher overall security and eliminates single points of failure. The following diagram illustrates the high-level architecture for VMware Cloud™ on AWS and the associated security responsibilities for both VMware and cloud tenants.



As outlined in the VMware Cloud on AWS Service Description, primary areas of responsibility between VMware and you are described below.

VMware Responsibility

- **Information security:** Protect the information systems used to deliver the Service over which we (as between VMware and you) have sole administrative level control.
- **Security monitoring:** Monitor for security events involving the underlying infrastructure servers, storage, networks and information systems used in the delivery of the Service Offering over which we (as between VMware and you) have sole administrative level control. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.
- **Patching and vulnerability management:** Maintain the systems we use to deliver the Service Offering, including the application of patches we deem critical for the target systems. We will perform routine vulnerability scans to surface critical risk areas for the systems we use to deliver the Service Offering. Critical vulnerabilities will be prioritzed.

FOURTEEN CLOUD SECURITY PRINCIPLES

1. Data in transit protection
2. Asset protection and resilience
3. Separation between users
4. Governance framework
5. Operational security
6. Personnel security
7. Secure development
8. Supply chain security
9. Secure user management
10. Identity and authentication
11. External interface protection
12. Secure service administration
13. Audit information for users
14. Secure use of the service

Customer Responsibility

- **Information security:** You are responsible for ensuring adequate protection of the Content that you deploy and/or access with the Service Offering. This includes, but is not limited to, selection of content you choose to put on the service, selection of the country in which you choose to store your content, any level of virtual machine patching, security fixes, data anonymization, masking and encryption, access controls, roles and permissions granted to your internal, external, or third-party users, etc.
- **Network security:** You are responsible for the security of the networks over which you have administrative level control. This includes, but is not limited to, maintaining effective firewall rules in all SDDCs that you deploy in the Service Offering.
- **Security monitoring:** You are responsible for the detection, classification and remediation of all security events that are isolated with your deployed SDDCs, associated with virtual machines, operating systems, applications, data, or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate and which are not serviced under another VMware security program.

Implementing Cloud Security Principles in VMware Cloud on AWS, the Cloud Security Guidance published by NCSC, lists 14 essential principles to consider when evaluating cloud services, and why these may be important to public sector organizations.

The 14 Cloud Security Principles, their objectives and how VMware Cloud on AWS can be used to implement these objectives are described below. The implementation of the controls necessary to comply with these principles are reviewed and attested to via third-party auditors who certify the VMware Cloud on AWS service is compliant with the ISO 27001, 27017 and 27018 standards along with other industry standards such as SOC 1, SOC 2 and HIPAA.

Cloud Security Principle 1: Data in transit protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

VMware Cloud on AWS implements multiple mechanisms to secure user data in transit. There are two options for securing data in transit to a customer's SDDC:

1. **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.
2. **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, Inc. (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.

Cloud Security Principle 2: Asset protection and resilience

User data and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure…

Physical location and jurisdiction

In order to understand the circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed.

VMware Cloud on AWS is hosted on AWS and leverages their globally available platform. When deploying a Software Defined Data Center customers have the ability to specify the specific AWS Region where the SDDC will reside, including AWS Europe (London).

Each AWS Region is made up of multiple Availability Zones which are designed for fault isolation by being connected to multiple Internet Service Providers (ISPs) and different power grids, while simultaneously being connected via high-speed links to enable Local Area Network (LAN) connectivity between Availability Zones within the same region.

A customer's workloads and data remain in that SDDC and are not moved unless the customer initiates a workload or data migration.

Data center security

Locations used to provide cloud services need physical protection against unauthorized access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data…

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.

Access privileges are promptly revoked when the employee or contractor no longer requires these privileges, regardless of their continued status as an employee of Amazon or AWS. When an employee is terminated, all access privileges are automatically revoked. As a further measure, all cardholder access to data centers is reviewed quarterly.

For more information on AWS controls and data centers, visit:

https://cloudsecurityalliance.org/starregistrant/amazon-aws/

https://aws.amazon.com/compliance/data-center/data-centers/

https://aws.amazon.com/compliance/data-center/controls/

Data at rest protection

To ensure data is not available to unauthorized parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media…

VMware Cloud on AWS provides multiple layers of encryption to ensure the security and integrity of the information customers store 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. This process is handled by the AWS API interface that VMware calls when allocating or deallocating host to a cluster. Encryption keys are generated in the SED controller and they never leave the drive.

Whenever a host machine is removed from a cluster the data encryption keys used by the self-encrypting drives are destroyed. This cryptographic erasure helps ensure that there is no Customer Content on the drives before returning the servers to the pool of available hardware.

The use of self-encrypting drives protects 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 provides storage array level encryption in addition to the existing VMware Cloud on AWS physical disk encryption found on NVMe self-encrypting drives. Encryption is implemented using XTS AES 256 cipher with Intel AES-NI, in both the cache and capacity tiers of vSAN datastores, for industry leading encryption with minimal impact on performance. vSAN enables data security benefits of encryption with no loss of deduplication & compression efficiencies.

The use of vSAN on top of the SEDs provides additional level of protection to VMware Cloud on AWS customers.

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.

In order to encrypt customer data, vSAN generates a Disk Encryption Key (DEK) used to encrypt the customer data and an intermediate key called local Key Encryption Key (KEK). The DEK is encrypted using the local KEK and the local KEK is in turn encrypted using the CMK.

The Key Encryption Key (KEK) and Data Encryption Key (DEK) are created by vSAN and stored in memory on each VMware ESX® host. DEKs are kept in ESXi memory to bootstrap vSAN disks and encrypt/decrypt the I/O data.

VMware chose to use the AWS KMS for vSAN encryption because of its security, availability and cost effectiveness. The AWS KMS service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of all customer keys. The plaintext keys never leave the HSMs unencrypted, are never written to disk and are only ever used in the volatile memory of the HSMs for the time needed to perform requested cryptographic operations.

- AWS KMS API endpoints receive client requests over an HTTPS connection using only TLS 1.2 or above. The API endpoints authenticate and authorize the request before passing the request for a cryptographic operation to the AWS KMS.
- The AWS Key Management Service provides for redundancy and failover within a single AWS region.
- AWS KMS keys are never transmitted outside of the AWS regions in which they were created.

Currently, there is no additional cost to the customer for use of encryption keys for VMware Cloud on AWS.

Key management

In order to meet industry or regulatory requirements, VMware Cloud on AWS customers can manage their keys by rotating the local KEK either through the vSAN API or through the vSphere UI. This process is called *shallow rekey*. A shallow rekey occurs instantaneously and is generally accepted method to rotate keys in order to comply with regulations.

Changing the Disk Encryption Key (DEK) and Customer Master Key (CMK) can be done by setting up a new cluster and moving VMs from the original cluster to the new cluster which encrypts the data using an entirely new CMK, KEK and DEK. This process may take several hours or days depending on the volume of data.

Customer managed encryption

Customers in need of an additional (third) level of encryption or who need to use their own keys or Key Management Infrastructure have the option to use any encryption or security software they wish within the guest operating system running on VMware Cloud on AWS. This offers flexibility and choice and enables customers to use the same security software they use in their own datacenters in the cloud.

Additional data security measures can be found in many popular databases, like Transparent data encryption (TDE), to enable encryption of sensitive data that is stored in tables and tablespaces. Many data protection products can be found in the VMware Cloud Marketplace.

FIPS 140-2 compliance

VMware has validated various cryptographic modules against the FIPS 140-2 standard for configuration of certain software products. The FIPS 140-2 standard specifies the cryptographic and operational requirements for the modules within security systems that protect sensitive information. These modules employ approved security functions such as cryptographic algorithms, key sizes, key management and authentication techniques.

VMware Cloud on AWS currently utilizes the latest validated version of vSphere which is has been validated through FIPS-140-2 process. The VM Kernel and OpenSSL modules utilized by vSphere version are certified and the certificates for each module can be found here:

VMware OpenSSL FIPS Object Module

VMware VMkernel Cryptographic Module

Currently only the VMware Cloud on AWS GovCloud instance of the service is configured to us the AWS KMS FIPS 140-2 validated endpoints and therefore is the only instance of our service that is truly FIPS compliant.

Data sanitization

The process of provisioning, migrating and de-provisioning resources should not result in unauthorized access to user data.

The VMware Cloud on AWS service helps ensure that whenever a host machine is removed from a cluster the data encryption keys used by the self-encrypting drives are destroyed. This cryptographic erasure helps ensure that there is no Customer Content on the drives before returning the servers to the pool of available hardware to be reprovisioned or decommissioned from service.

Equipment disposal

Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service or user data stored in the service.

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 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.

Physical resilience and availability

Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business…

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. A Risk Assessment is performed on a regular basis to identify natural and manmade threats based upon a geographically specific business impact assessment. Reviews are triggered through change management, new projects, and critical process reviews. The resulting 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 architecture of AWS provides tremendous redundancy such that customers who run their workloads in multiple regions are effectively operating across multiple providers.

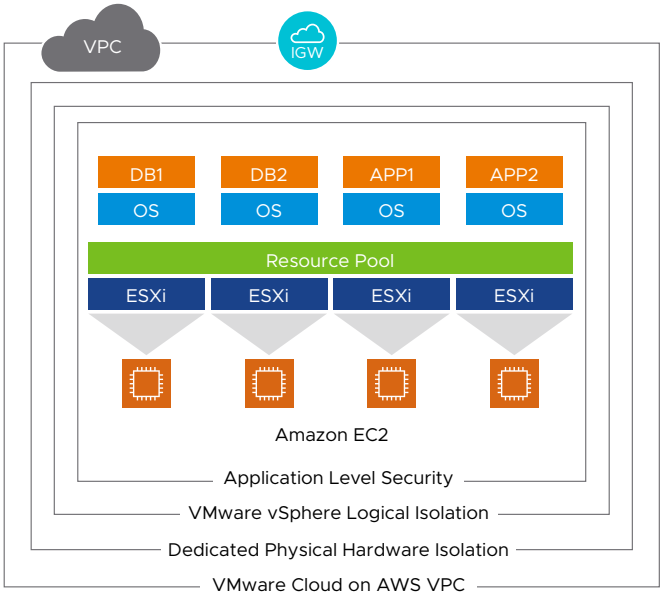
As a part of the VMware Business Impact Analysis, dependencies on third parties are documented to ensure appropriate business continuity measures are in place.

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, including ISO 27001. VMware will furnish audit reports under NDA as they become available.

Cloud Security Principle 3: Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another.

The VMware Cloud on AWS service has four independent layers of separation between customer environments. Each layer offers industry leading levels of security and combined, they provide customers with the most secure cloud service.



Dedicated AWS account and VPCs

Each VMware Cloud on AWS customer SDDC is deployed using a dedicated AWS account and within its own AWS Virtual Private Cloud (VPC). This is how AWS logically isolates its customers. This level of separation in itself has been recognized as highly secure by most security organizations and industry standards.

Dedicated EC2 bare metal instances – physical separation

Every customer SDDC deployed within an AWS VPC is deployed on dedicated Bare Metal EC2 hardware. This provide a physical separation between each customer that ensures that there are no other customers leveraging the local compute, memory or storage resources. This protects against customers competing for virtual hardware resources and also against exploitation of physical hardware vulnerabilities.

Additionally, customers who choose to run I3 instances in their SDDC store their content on dedicated local self-encrypting NVME drives which helps eliminate concerns over potential security issues with shared storage.

VMware Software Defined Data Center (SDDC)

On top of the deployed physical servers, VMware runs our industry leading virtualization platform. The VMware Cloud on AWS SDDC includes vSphere, vSAN and NSX® and offers an additional layer of logical isolation. VMware's products have been leveraged by customers for over 20 years to run multi-tenant environments and are considered to be highly secure by themselves.

VMware vSphere provides a third layer of separation via logical isolation using Virtual Machines and Resource Pools. vSphere also provides security features including Encryption, Access Management and permissions, as well as comprehensive logging capabilities that allow customers to monitor access and changes to the virtual environment – including changes at the hypervisor level.

Operating system and application level security

Finally, With VMware's industry proven compatibility and broad ecosystem supporting application and partner products, VMware Cloud on AWS allows customers to run their own tools to implement additional levels of separation.

These can be deployed in a manner similar to what they run on-premises. Customers can implement operating system or application level access controls and polices, enable encryption and install third-party tools that provide additional security and monitoring capabilities.

Cloud Security Principle 4: Governance framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined…

In alignment with the ISO 27001 standard, VMware maintains a Risk Management program to mitigate and manage risk companywide. Risk assessments are performed at least annually to ensure appropriate controls are in place to help reduce the risk related to the confidentiality, integrity and availability of sensitive information.

VMware Cloud Services management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. VMware Cloud Services management reevaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

Executive and senior leadership, led by the VMware Chief Information Security Officer, play important roles in establishing the Company's tone and values as it relates to information security. The Information Security and Compliance teams, together with management, are responsible for maintaining awareness and complying with security policies.

Business Conduct Guidelines and Security Awareness training is required for employees both upon hire and annually. VMware provides security policies and security training to employees to educate them about their role and responsibilities concerning information security. Employees who violate VMware standards or protocols are subject to appropriate disciplinary action. Applicable security provisions are added to supplier agreements to ensure providers are contractually obligated to maintain appropriate security provisions. These policies are reviewed as part of the VMware audit and assessment program. VMware third-party auditors also perform reviews against industry standards, including ISO 27001.

VMware has documented security baselines to guide personnel in ensuring that appropriate configurations are in place to protect sensitive information. Baseline configurations for all software and hardware installed in the production environment are documented and updated regularly. Changes are governed by a defined change management policy, with baseline configurations securely recorded.

Cloud Security Principle 5: Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

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.

The scope of these standards applies and extends to information systems and applications that are owned, managed and/or operated by VMware, in both VMware and third-party data centers and cloud environments; as well as to all business processes associated with the operation of these information systems and applications; and to all VMware employees, consultants, contractors, agents, and vendors who manage or operate VMware information systems and applications and/or business processes.

Configuration and change management

You should have an accurate picture of the assets which make up the service, along with their configurations and dependencies.

VMware follows a strict policy of security baseline configuration that includes pre-implementation approvals and alignment with standards set by USGCB, FDCC, DISA, STIGs and CIS Benchmarks. All security baseline configuration changes are reviewed for approval in a timely manner. The Vulnerability Management team also maintains a central repository of security baseline configurations to satisfy legal/regulatory requirements.

Vulnerability management

Service providers should have management processes in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools.

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.

Protective monitoring

A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of your environments and data.

VMware Cloud on AWS benefits from AWS's employment of various technologies that monitor configuration changes in the cloud infrastructure in near real-time (collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes). Additional capabilities are used to block network attacks (DDoS, MITM, IP Spoofing and port scanning) through Internet access diversity, SSL protected endpoints, SSH host key regeneration, restrictive host-based firewall infrastructure, and reactive scanning detection backed by a strictly enforced Acceptable Use Policy.

The cloud control plane supporting VMware Cloud on AWS is hosted on Amazon Web Services, Inc. (AWS) and is protected 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.

Incident management

Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users…

VMware's Vulnerability Management Policy includes processes to identify, report, and remediate information security vulnerabilities; to manage vulnerability remediation exceptions; review and analyze vulnerability remediation exceptions on a regular basis; test software and firmware updates related to security flaws to evaluate effectiveness and identify potential impacts prior to implementation; install the most recent stable versions of applicable security software and firmware updates in a timely manner; and to verify the source and integrity of the patch. VMware ensures patches are tested in an environment that closely approximates the production environment.

We have the VMware Cloud status page to communicate the status of any outages or incidents for the Service Offering.

Cloud Security Principle 6: Personnel security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

VMware has established screening procedures for all employment candidates, which includes background checks on the following: social security number verification, employment history verification, education verification, and a criminal background check. New hires attend orientation meetings to review corporate security policies and obligations.

A quarterly access review audit is performed to ensure service access is still appropriate. Controls are in place to ensure the timely removal of systems access that is no longer required for business purposes. HR systems, policies, and procedures are in place to help guide management during termination or change of employment status. Access privileges to systems are removed when an employee leaves the company. An employee who changes roles within the organization will have access privileges modified according to their new position.

The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.

AWS also conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees. As part of the on-boarding process, all personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy. Additionally, AWS maintains employee training programs to promote awareness of AWS information security requirements, including periodic Information Security training and compliance audits to validate that employees understand and follow the established policies.

Cloud Security Principle 7: Secure development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity...

VMware has invested in the Security Development Lifecycle (SDLC) process which is continuously evolving in response to the threat landscape and a security organization that utilizes multiple key resources to ensure that VMware Cloud Services implements appropriate operational and security controls.

The SDLC program is designed to identify and mitigate security risk during the development phase of VMware software products so that the development group's software is safe for release to customers. Code undergoes rigorous review for code security and quality. The VMware Product Security and product development groups apply the methodology as an end-to-end set of processes to use at specific times in the development group's software development lifecycle, with the goal of helping teams to remediate any security issues early in the lifecycle.

As part of the SDLC, VMware uses both manual and automated source code analysis tools to help detect security defects in code as well as security vulnerabilities in applications prior to production. Vulnerabilities posing a significant risk are addressed prior to deployment.

VMware SDLC and change management processes guide personnel to ensure appropriate reviews and authorizations are in place prior to implementing any new technologies or changes within the production environment. Change management policies and processes are also in place to guide management authorization of changes applied to the production environment. Internal audits of these processes are performed under the VMware Information Security Management System (ISMS) program and are essential to the VMware continuous improvement programs.

Additionally, the VMware Acceptable Use Policy prohibits the use of unauthorized software. Production servers are provisioned and managed programmatically via Infrastructure as Code software. No software can be installed on these systems manually or without several reviews and approvals. Additionally, continuous monitoring by VMware Cloud Services system monitoring tools is in place to detect unauthorized changes.

Cloud Security Principle 8: Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all the security principles which the service claims to implement.

VMware customers retain control and ownership over the quality of their data and potential quality errors that may arise through their usage of VMware Cloud Services. Access privileges to VMware systems is based on an individual's "need to know," as determined by job functions and requirements. Access privileges to computers and information systems is authorized by the appropriate level of management and documented prior to being granted. Managing access to information systems is implemented and controlled through centralized identity stores and directories.

Internal audits are performed at least annually under the VMware information security management system (ISMS) program. VMware uses internal and external audits to measure the conformance and effectiveness of the controls applied to reduce risks associated with safeguarding information and to identify areas for improvement. Audits are essential to the VMware continuous improvement program.

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 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 ensure appropriate controls are in place to 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.

Cloud Security Principle 9: Secure user management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorized access and alteration of your resources, applications and data.

Identity and access management controls are in place within VMware Cloud Services environments to restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems, and to help ensure appropriate personnel have the appropriate level of access.

Access to, and use of, audit tools that interact with an organization's information systems is appropriately segmented and restricted to prevent compromise and misuse of log data. Strict access control, separation of duty, and other policies define which individuals have access to VMware management systems.

All critical systems access is logged and monitored. Privileged access is logged and captured in a centralized log server. SIEM tools are used to monitor logs by the VMware Security Operations Center. Customers are responsible for managing access to the administrative console and end-user access via their RBAC (Role Based Access Control) and Identity Management Access System. Customers also maintain control of who has access to their VMware Cloud Services and virtual network controls and who can use a local directory service or federate to a corporate directory service.

Access to diagnostic and configuration ports is restricted to authorized individuals and applications. VMware systems management access is performed over a dedicated network connection. Customer management access is performed over a dedicated management network connection that is established over a VPN.

VMware access control is implemented via directory services group management where all individuals who have access to the IT infrastructure and network and their level of access can be identified by enumerating the members of these dedicated groups.

Internal corporate or customer (tenant) user account credentials are restricted, helping ensure appropriate identity, entitlement, and access management, and in accordance with established policies and procedures. VMware supports use of, or integration with, existing customer-based single sign-on (SSO) solutions to our service.

Cloud Security Principle 10: Identity and authentication

All access to service interfaces should be constrained to authenticated and authorized individuals…

VMware provides identity and access management controls that restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems, and to ensure users have the appropriate level of access. Strict access control, separation of duty, and other policies define which individuals have access to VMware management systems.

All critical systems access is logged and monitored. Internal corporate or customer (tenant) user account credentials are restricted, ensuring appropriate identity, entitlement, and access management, and in accordance with established policies and procedures. VMware supports use of, or integration with, existing customer-based single sign-on (SSO) solutions to our service.

Access to tightly controlled audit tools that interact with the organization's information systems is appropriately segmented and restricted to prevent compromise and misuse of log data. Similarly, access to diagnostic and configuration ports is restricted to authorized individuals and applications. VMware systems management access is performed over a dedicated network connection.

VMware also provides lifecycle management of customer keys. Key management policies and procedures are in place to guide personnel on proper encryption key management. Access to cryptographic keys is restricted to named personnel and all access is logged and monitored. Cryptographic keys used by self-encrypting drives are managed by Amazon Web Services. All keys used in VMware Cloud Services are unique to each customer. Customer-specific keys are programmatically generated by an independent and well-established certificate authority at the time of provisioning and are tied to the unique URLs created for each tenant. VMware has key management controls in place and personnel to manage and secure the encryption

certificates used to communicate with the VMware Cloud Services consoles. VMware Cloud Services operations have complete visibility into certificate information such as installed, expiring and revoked certificates through a certificate management dashboard. Amazon Web Services manage the keys used by self-encrypting drives.

Cloud Security Principle 11: External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended…

Managed interfaces are configured to help deny communications traffic by default and allow network communications traffic by exception.

Data input to the VMware Cloud on AWS is limited to account information that primarily consists of system configuration information that must match expected inputs or formats. The product interfaces and services enforce the integrity of the information, and validation is accomplished via real-time service execution where possible. All input and output processing of customer data is the responsibility of the customer.

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 Services has established an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information.

VMware Cloud on AWS also benefits from AWS's built-in protections, which include network devices that monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet Service Providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices.

Cloud Security Principle 12: Secure service administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data…

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 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.

The Terms of Service and Data Privacy Addendums for the VMware Cloud Services establish the line of demarcation between the responsibility of VMware and those of

the customer as it pertains to data protection. Additionally, information is available to customers to establish transparency regarding the separation of responsibility between VMware and the customer for compliance programs or data privacy rules.

Cloud Security Principle 13: Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales…

Customer SDDC logs: 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.

a. The Audit logs collected by VMware Cloud on AWS are specific to the administrative operations that are conducted by administrators using the VMware Cloud Console and vCenter to configure and manage customer networks and their workload VMs. The logs collected by VMware Cloud on AWS also track the administrative actions of VMware Support team activities. All logs are forwarded to the vRealize® Log Insight™ Cloud customer tenant and the VMware Support tenant for troubleshooting purposes.

b. The Audit logs collect limited information about the customer administrator date & time, login id, ip.. (see vRLIC Field List)

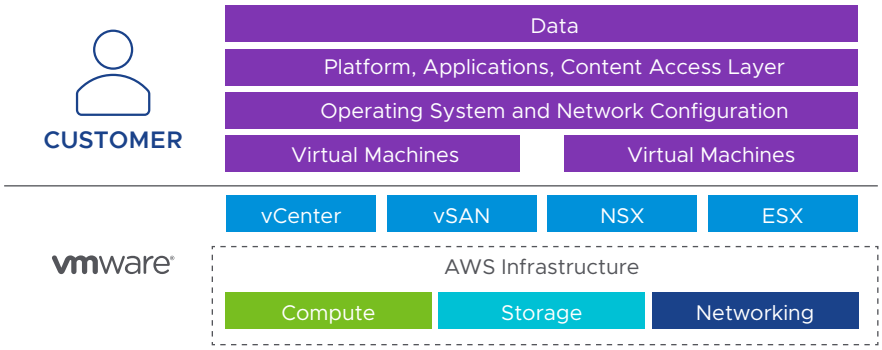
c. The monitoring logs collect information and telemetry metrics relative to the performance and health of the SDDC infrastructure.

Backend Infrastructure logs: These are collected across the VMware infrastructure and supporting SaaS services platforms. Each individual system within the larger VMware cloud platform sends the collected audit logs to a centralized log storage location with a secure storage policy. The audit logs are then collected by a secured logging pipeline that sends the audit logs into a SIEM that is managed by the VMware employee managed Security Operations Center (SOC). The lifecycle for all audit logs have a retention period of three years. The storage policies applied to audit logs are monitored by the VMware SOC and alerts are generated if the policy is violated or any attempts to change the policy that protects the storage.

Cloud Security Principle 14: Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

VMware operates on a Shared Responsibility model where responsibilities are clearly defined among Customer, VMware and AWS.



Customer responsibility "Security in the Cloud" – Customer responsibility is determined by the VMware Cloud on AWS services that you select. In addition to determining the configuration work you need to perform as part of your security responsibilities, customers are responsible for managing data (including encryption options), classifying assets, and using IAM tools to apply the appropriate permissions.

- **VMware responsibility "Security of the Cloud"** – VMware is responsible for protecting the infrastructure that runs all of the services offered in VMware Cloud on AWS. This infrastructure is composed of the hardware, software, networking, and facilities that run VMware Cloud on AWS services.
- **AWS responsibility "Security of the Infrastructure"** – AWS is responsible for the physical security, infrastructure and hardware underlying the entire service.

The VMware and customer shared responsibility model also extends to Security and compliance controls. Like how the responsibility to operate the IT environment is shared between VMware Cloud on AWS and customers, so is the management, operation and verification of IT controls. VMware Cloud on AWS helps relieve the burden of operating controls by managing those controls associated with the physical infrastructure deployed in the environment – controls that may previously have been managed by the customer. Because every customer is deployed differently in VMware Cloud on AWS, each can take advantage of the shift in management of certain IT controls to VMware, resulting in a distributed control environment. Customers can then use the available VMware Cloud on AWS control and compliance documentation to perform control evaluation and verification procedures as required by their organizations.

Note: The information provided in this document is provided "AS IS" without warranty of any kind. This documents does not amend or supplement any license, support or service agreement you may have in aplce with VMware.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Item No: Fourteen Cloud Security Principles 04/2020