WHITE PAPER–AUGUST 2019

VMware Cloud Services Security Overview

An in-depth view of VMware's approach to cloud security

vmware®

Table of contents

Overview 4
- Driving principles 4
- Shared responsibility 5
- VMware Cloud Services security framework 6

Physical and management layer security 7
- Physical security 7
- Management layer 7

Code security. 8
- Application and interface security 8
- Change control and configuration management 8

Data security 9
- Internal standards and policies 9
- Interoperability and portability 9
- Data classification, handling and labeling 9
- Production and non-production environments 10
- Customer data access by VMware 10
- Data location 11
- Data protection 11
- Data integrity 12
- Backups 12
- Secure disposal 12

Network security 13
- Segmentation 13

Identity and access management 14
- Customer access requirements 14
- Users, groups and roles 14
- User access reviews and revocation 15
- User ID credentials 15
- Key management 16

Vulnerability and patch management 17
- Antivirus and malicious software 17

Operations management 18
Security, logging, monitoring and intrusion detection 18
Incident reporting 19
Security support processes 20
Human resources 20
Asset management 22
Governance, risk and compliance 23
Risk assessments, program management and policy 23
Supply chain management, transparency and accountability 23
Audit assurance and compliance 24
Enterprise resilience 25
Business continuity 25
Disaster recovery 25
Conclusion 26

Overview

This document provides a general overview of the security controls implemented in various VMware Cloud™ Services offerings that run on the Amazon Web Services infrastructure as a service (IaaS). The intent is to provide readers with an understanding of how VMware approaches security for its cloud offerings, the key mechanisms and processes VMware uses to manage information security, and insight into the shared responsibility for providing security in a modern cloud computing environment.

Please note: This document only covers those VMware Cloud Services offerings that run on the Amazon Web Services IaaS.

Driving principles

Security of VMware Cloud Services is of utmost importance. Ensuring the security of VMware Cloud offerings and the customer data held within requires a wide array of tools, processes and capabilities, all expertly designed to balance the desires of the business with a focus on customer satisfaction, product efficiency, product deadlines, revenue, and shareholder expectations and the need for security. VMware balances these needs with a set of controls and management processes designed to mitigate risk and enhance its product offerings.

The controls and processes were created using a set of driving principles, which provide the underlying general rules and guidelines for security within VMware Cloud Services:

- Risk – Manage risk by understanding the threat landscape, building a solid platform and leveraging all decision-makers when calculating risk.
- Controls – Establish a balance of effectiveness and efficiency by implementing the appropriate controls for the associated risk.
- Security – Provide preventative and protective capabilities to ensure a secure service.

Shared responsibility

VMware Cloud Services uses a shared responsibility model for security. Trusted security in the cloud is achieved through the partnership of shared responsibilities between customers, VMware and Amazon Web Services. This matrix of responsibility ensures a higher security model and eliminates single points of failure. Figure 1 illustrates the high-level architecture for VMware Cloud Services and the associated security responsibilities for both VMware and cloud tenants.

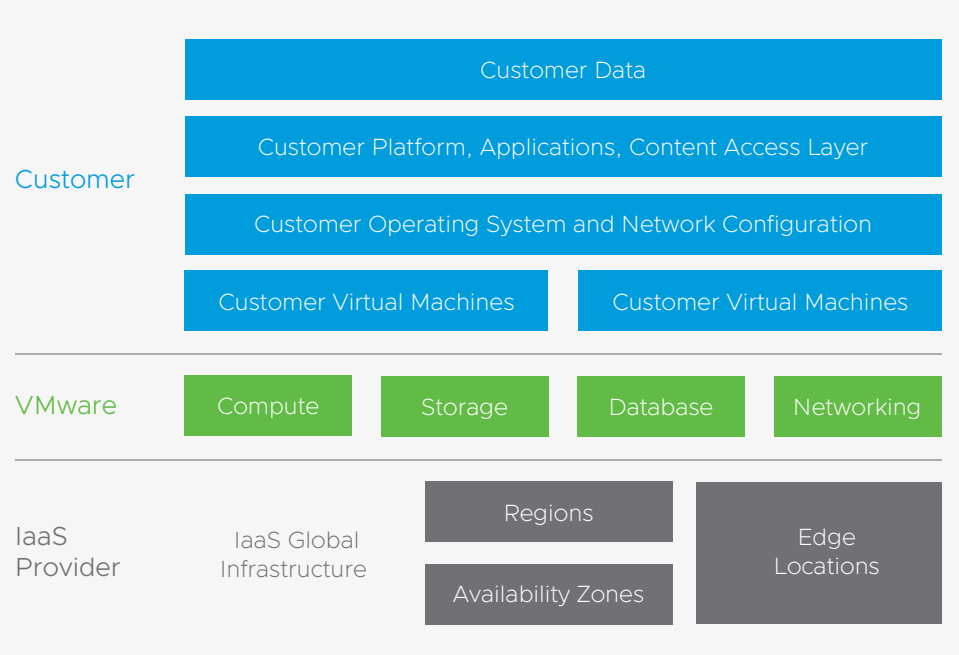

FIGURE 1: VMware Cloud Services architecture.

VMware delivers the service, Amazon Web Services delivers the underlying infrastructure, and customers consuming the service share responsibility within the overall security landscape for services run on VMware Cloud Services. Amazon Web Services is responsible for the security of the underlying physical infrastructure of the data center across all regions and availability zones as well as edge locations. VMware is responsible for ensuring all facets of security for the management layer. And customers continue to own and operate the security and compliance of the actual workloads by extending their successful policies and controls to public cloud locations.

VMware Cloud Services security framework

To provide focus for VMware's security responsibilities as a cloud service provider, we established a security framework. This framework helps abstract the levels of detail typically found in security implementations, categorize the control elements and frame the elements in a meaningful order.

FIGURE 2: VMware security framework.

The remainder of this document details each element of the framework, describing key controls implemented in VMware Cloud Services.

Physical and management layer security

Physical security

In a cloud environment, solid compute, storage and network security is only as effective as the security of the physical environment used to house the infrastructure.

VMware Cloud Services offerings run on physical infrastructure built and maintained by IaaS cloud service providers such as Amazon Web Services, Microsoft Azure, Google Cloud Platform and SoftLayer. This infrastructure leverages data centers that have physical security controls including, but not limited to, perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems, as well as other electronic means such as two-factor authentications to access data center floors. The physical infrastructure used by VMware Cloud Services varies depending on the offering.

Each individual VMware Cloud Services offering will identify the IaaS provider that is used.

Management layer

The management layer provides the controls for operating the cloud service infrastructure used to deliver VMware Cloud Services. VMware uses dedicated secure networks when accessing the management software used to operate the infrastructure. Only authorized personnel involved in the operation and maintenance of VMware Cloud Services have access to this management network. Access by these teams is managed with multiple levels of access controls before accessing VMware Cloud Services infrastructure.

Code security

VMware has well established controls in place to protect all application, program or object source code, and to assure it is restricted to authorized personnel only.

Application and interface security

VMware has an industry-leading security development lifecycle process and a world-class security organization that focuses on ensuring VMware Cloud Services implements industry-standard operational and security controls.

The security development lifecycle 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 a 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 these security issues early in the lifecycle.

As part of the security development lifecycle, VMware uses both manual and automated source code analysis tools to detect security defects in code as well as security vulnerabilities in applications prior to production. Critical vulnerabilities are addressed prior to deployment.

VMware verifies that all software suppliers adhere to industry standards for security development lifecycle security using its comprehensive vendor risk management process that includes review of our vendor's security controls, development processes, privacy controls, business conduct, and third-party audit reports and certifications.

Change control and configuration management

VMware's security development lifecycle 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.

VMware Cloud Services does not outsource software development activities and has a comprehensive testing system that covers the entire lifecycle of the release. Continuous testing occurs on the software development pipelines for individual products and components. VMware generates builds from approved components and runs these through basic integration tests (BITs), product validation tests (PVTs), feature stress lite (FSLite) tests, and continuous loop tests for deployment, upgrade and cluster expansion/reduction across all supported regions. Additionally, VMware runs performance tests, feature stress tests, security scans, vulnerability tests and system tests at scale for every cycle. Product bugs follow a standardized process for capture, investigation, development, testing, change approval and implementation. Vulnerabilities are handled through the VMware vulnerability management procedures.

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.

Known issues are provided publicly in VMware product and service release notes.

Data security

Internal standards and policies

Internally, VMware has a data handling and protection standard in place to guide employees on appropriate labeling and handling for each classification level. Handling procedures include the classification, processing, storage, transmission and destruction of data.

As part of the risk management process, controls are implemented to mitigate and contain data security risks. This includes the use of separation of duties, role-based access control and least-privilege access for all personnel in the supply chain. VMware's risk management process also includes an accounting of supply-chain partner data quality errors, associated risks and appropriate corrective action policies.

Interoperability and portability

VMware maintains and publishes a comprehensive list of APIs that customers can use to verify interoperability between components and facilitate migrating applications.

Data classification, handling and labeling

VMware Cloud Services follows a data-labeling standard in addition to having data classification guidelines. VMware has a data handling and protection standard in place to guide employees on appropriate labeling and handling for each classification level. Handling procedures include the secure processing, storage, transmission, declassification and destruction of data. All account information is processed according to these guidelines.

Customers retain control and ownership of their customer content, and it remains the responsibility of customers to implement a structured data-labeling standard to meet their requirements if they so choose.

Production and non-production environments

The VMware software development and release processes contain well-defined mechanisms in place to ensure that the non-production code is removed or disabled before release or deployment into production.

VMware's infrastructure is partitioned into production and non-production environments. VMware Cloud Services development is performed in non-production environments with documented procedures for testing and validation of updates prior to production release. The VMware Cloud Services production environments contain the underlying infrastructure management software, customer data and customer virtual machines.

Production and non-production environments are logically and physically segregated. Development, quality assurance (QA) and production use separate equipment and environments, and are managed by separate teams.

Production data is not replicated or used in non-production environments.

Customer data access by VMware

Customers retain control and ownership of their customer content, and data stewardship of customer data remains the responsibility of the customer.

Access privileges to VMware systems are controlled based on the principle of least privilege—only the minimum level of access required shall be granted. Access is based on an individual's need to know as determined by job functions and requirements. Access privileges to computers and information systems are 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.

Access to customer environments where a customer's data is stored requires an authorized VMware operator to authenticate via two-factor authentication to an access control system to generate a user-specific time-based credential. Generation of these temporary credentials must be tied to a specific incident, and all activity performed by the users is logged. The VMware Security Operations Center uses log capture, security monitoring technologies and intrusion detection tools to monitor VMware personnel accessing customer data and to look for unauthorized access attempts.

All access to customer data is logged and disclosed to the customer via the service interface. Processes and procedures are in place to ensure management authorization is in place prior to access provisioning. No third parties have access to the production environment or customer content. If customers have questions about a specific individual accessing their environment, VMware will work with the customer to investigate the activity.

Data location

Customers choose the physical data center where they want their data deployed, and data is not moved away from that physical data center unless data migration is performed by the customer or the customer purchases an offline data transfer offering. Customers may place workloads and store data within one or multiple geographic regions based on which location(s) best suits their needs. Customer content does not traverse locations without the explicit actions of the tenant administrator. Documentation exists describing the use of supporting migration and replication technologies. It is the customer's responsibility to implement their workloads in a highly available manner for VMware Cloud Services offerings.

Data protection

For data that is required to move through public networks, VMware provides customers with the ability to create IPsec and SSL VPN tunnels from their environments that support the most common encryption methods, including 128-byte and 256-byte AES. Data in transit (authentications, administrative access, customer information, etc.) is encrypted with standard encryption mechanisms (i.e., SSH, TLS and Secure RDP). Communication that transports sensitive information (authentications, administrative access, customer information, etc.) is encrypted with standard encryption mechanisms.

Data integrity

Data input to VMware Cloud Services 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 ISMS based on ISO 27001 standards to manage risks relating to confidentiality, integrity and availability of information.

Backups

VMware does not back up or archive customer data.

Secure disposal

Exiting the VMware service is highlighted in the service description. Following expiration or termination of the service, the customer is responsible for removing or deleting their customer content. VMware will cooperate with the customer to delete or return all customer content as provided in the customer agreement except to the extent VMware is required by applicable law to retain some or all of the personal data, in which case VMware will archive the data and implement reasonable measures to prevent the customer content from any further processing.

Network security

VMware Cloud Services relies on layers of network security and builds on top of the base network security provided by Amazon Web Services. Customers have access to documentation and user guides as well as technical support, a knowledge base and other technical assets. Additionally, professional services are available for purchase. Customers may also reference white papers and other information instructing them on how to properly secure virtual environments.

Network architecture diagrams that include data flows between security domains/zones are updated regularly. Audits are regularly performed to review the appropriateness of the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network.

Policies, procedures and configurations are in place to protect VMware network environments. Wireless networks are not used to connect directly to the production environment.

Network diagrams and data flows are in place that clearly identify high-risk environments and systems that may have legal compliance impacts. VMware has implemented technical measures and applies defense-in-depth techniques for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or distributed denial-of-service (DDoS) attacks. VMware has security controls in place to reduce the risk of unauthorized access to sensitive information in the production environment. VMware Cloud Services has several intrusion detection mechanisms in place, and continuously collects and monitors the environment logs correlated with both public and private threat feeds to spot suspicious and unusual activities.

Segmentation

VMware Cloud Services has logically separated networks that restrict the customer's access to their own private networks. The system and network environments are protected by a firewall or virtual firewall to ensure business and customer security requirements, as well as 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 to support the protection of VMware information systems.

The Terms of Service and Data Privacy Addendums for 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.

Identity and access management

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 ensure appropriate personnel have the appropriate level of access. These controls are based on the principle of least privilege.

Customer access requirements

Prior to granting access to VMware Cloud Services, customers are required to review and agree to a Terms of Service that is made publicly available to prospects and customers.

Users, groups and roles

Access to and use of audit tools that interact with the 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's management systems.

All critical systems access is logged and monitored. Privileged access is logged and captured in a centralized log server. The VMware Security Operations Center uses security information and event management (SIEM) tools to monitor logs.

VMware has established human resources (HR) policies for terminated employees. 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 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.

Customers are responsible for managing access to the administrative console and end-user access to customer resources. Customers also maintain control of who has access to their VMware Cloud Services environment and virtual network controls, and 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 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.

The *Terms of Service*, service description and documentation outline the lines of demarcation between VMware's responsibilities, the segregation of duties within VMware, the responsibilities of Amazon Web Services and the customer's responsibilities.

User access reviews and revocation

A quarterly access review audit is performed to ensure certification of entitlements for all VMware Cloud Services critical system users and administrators. All entitlement actions, along with remediation and certification actions for inappropriate entitlements, are recorded via the systems used to grant/revoke access. User access reviews, along with user entitlement remediation and certification, are audited and reviewed as part of the annual independent third-party assessments, and reports will be shared when these assessments are made available to our customers. Third-party auditors will perform reviews against industry standards, including ISO 27001. VMware will furnish audit reports under a non-disclosure agreement (NDA) as they become available.

When it comes to user access revocation, there is timely de-provisioning (revocation or modification) of user access to the organization's systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties. VMware has HR systems, policies and procedures in place to help guide management during termination or change of employment status. Access privileges to systems are removed with a status change. Employees or contractors who change roles within the organization will have access privileges modified according to their new position. Any change in user access status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization. A quarterly access review audit is performed to ensure access is still appropriate, and regular internal audits are conducted to confirm access control changes have been implemented on critical systems.

User ID credentials

Internal corporate or customer (tenant) user account credentials are restricted to ensure the appropriate identity, entitlement and access management, and to be 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.

There are also mechanisms in place for unlocking accounts that have been locked out. For system accounts, the VMware self-service password reset interface will email a time-limited, one-time password to the customer to the email address on record. For federated solutions, password reset processes are the responsibility of the customer.

Key management

Lifecycle management of customer keys that are managed by VMware is documented. 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 per 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 manages the keys used by self-encrypting drives.

VMware uses an industry-leading commercial solution to secure, store, and tightly control access to tokens, passwords, certificates, API keys and other secrets. In addition, VMware certificate vendors have certificate management dashboards that can be used to monitor and manage the certificates that VMware is responsible for. Both of these encryption key management systems have been augmented by a VMware-built application to monitor and automate the management of the keys for the service.

VMware Cloud Services leverages encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances. For VMware Cloud Services offerings that enable transport from on-premises environments to the VMware Cloud Services environment, all information is sent over a VPN connection. One of these offerings is VMware HCX®, which facilitates the bulk migration of data. This service uses AES-256 encryption to encapsulate in-transit workloads. For in-cloud VMware HCX vMotion® activities, a dedicated, secure and encrypted network is used.

Vulnerability and patch management

Network layer, application, and internal or local operating system layer vulnerability scans are performed regularly as prescribed by industry best practices as part of the vulnerability management program. VMware's comprehensive vulnerability management program includes third-party vulnerability scanning and penetration testing. Results of vulnerability scans are not shared with customers as they do not participate in the vulnerability management program of the service. This helps to ensure the confidentiality, integrity and availability of our hosted offering. Vulnerability scans are reviewed as part of the annual audit and assessment program.

VMware patches or upgrades all network, utility and security equipment after analyzing the severity and impact of potential vulnerabilities. VMware has subscriptions to pertinent vendor security and bug-tracking notification services. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical patches are installed in a timely manner. Non-critical patches are included in the pre-defined patch schedule and applied within commercially reasonable timeframes. Changes are made using industry best practices. Patch testing and rollback procedures are completed by the QA department to ensure compatibility with and minimal impact to the production environment.

Third-party auditors will perform reviews of the vulnerability and patch management process against industry standards, including ISO 27001. VMware will furnish audit reports under an NDA as they become available.

Antivirus and malicious software

Anti-malware programs are installed if components typically vulnerable to malware are used within the service. Security threat detection systems and anti-malware systems are configured and updated across all infrastructure components based on industry-accepted timeframes.

Operations management

Security, logging, monitoring and intrusion detection

Higher levels of assurance are required for the protection, retention and lifecycle management of audit logs. This ensures audit logs adhere to applicable legal, statutory or regulatory compliance obligations; provide unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies; and support forensic investigative capabilities in the event of a security breach.

The service continuously collects and monitors the environment logs, which are correlated with both public and private threat feeds to spot suspicious and unusual activities. Furthermore, intrusion detection devices such as honeypots are used.

Physical and logical user access to audit logs is restricted to authorized personnel. Restricted, authorized personnel have access to the definitive central log servers for the VMware Cloud Services servers. The customer's access logs are replicated to other systems where they can be viewed by customers and other individuals with appropriate approvals.

Audit logs are centrally stored and retained whenever required. They are tested annually by the ISMS, and are monitored and reviewed for security events by the VMware Security Operations Center 24 hours a day, 7 days a week.

VMware has an intrusion detection system and other tools in place that continuously monitor for deviations in production from our baseline configurations and generate notifications.

Security incident management

The VMware Incident Response program's plans and procedures have been developed in alignment with the ISO 27001 standard. For the purpose of security and incident management, VMware maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. Points of contact are regularly updated to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.

Under the VMware ISMS program, the incident response plan is tested at least once annually, whether or not a security incident has occurred.

Incident reporting

The logging and monitoring framework for VMware Cloud Services allows for the identification of incidents to specific tenants. A SIEM system is in place and merges data sources for granular analysis and alerting, and is used by the VMware Security Operations Center.

VMware has a formal incident response group that facilitates all incident response activities. Forensic data can be made available for third-party forensic analysis, if required by law. VMware analyzes information security risk impact based on internal mechanisms to quantify the types, volumes and impacts on all information security incidents. VMware considers these policies and procedures to be internally confidential and cannot share specific details with customers. Information pertaining to security breaches will be shared with affected customers in support of VMware's contractual and legal obligations. VMware will notify the customers through electronic methods (e.g., portals) where feasible.

Please reference the *VMware Data Processing Addendum* for more information.

Integrity

VMware ensures the integrity of all virtual machines' images at all times. All infrastructure actions are logged in the service, and alerts are raised regardless of their running state. Images are not moved without the explicit actions of the tenant administrator. All changes or movement of an image is immediately noted in the log files, which are available to the customer. Additionally, the notifications are available through alerts and portals. Implementation of integrity checking on a customer's virtual machine images is the responsibility of the customer.

Security support processes

Human resources

Background screening

Pursuant to local laws, regulations, ethics and contractual constraints, all employment candidates, contractors and involved third parties are subject to background verification. VMware conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to the service. Independent audit reports will provide additional details regarding the controls in place for background verification.

Employment agreements, training and termination

In alignment with the ISO 27001 standard, all VMware personnel are required to complete annual security awareness training. Personnel supporting VMware managed services receive additional role-based security training to perform their job functions in a secure manner. Compliance audits are periodically performed to validate that employees understand and follow the established policies. All VMware personnel are required to sign confidentiality agreements as part of onboarding. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the VMware Business Conduct Guidelines.

An enterprise learning management system is used to facilitate the delivery of VMware training programs, including the annual security awareness training, which is required for access to sensitive systems. All personnel who have access to VMware services must undergo the referenced annual security awareness training. The tools used record the successful completion of required training, and completion reports are reviewed during ISMS review meetings. Personnel who have access to our production environment receive additional training as they assume job roles and responsibilities within their specific department. This training is completed before authorizing access to production systems.

All VMware personnel are required to sign employment agreements to ensure all customer/tenant information is kept confidential. Applicable policies are reviewed at planned intervals by VMware. 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. Terminated employees are required to return assets.

Roles and responsibilities of contractors, employees and third-party users are documented as they relate to information assets and security. The VMware Cloud Services *Universal Terms of Service*, service descriptions, privacy addendums and service documentations outline the line of demarcation between the customer's responsibilities and those of VMware.

The VMware *Data Processing Addendum*, *Privacy Policy* and Terms of Service disclose to customers what type of usage data is collected during their use of the service. This includes data such as information on the amount of computing and storage resources purchased or consumed, named user counts and third-party licenses consumed. VMware does not allow tenants to opt out of having their data/metadata accessed via inspection technologies. The type of data VMware collects is outlined in our Data Privacy agreement, and the methods by which we use the data is clearly stated and available publicly on our website. This collection of the types of data specified are necessary for us to deliver the services outlined by our service description.

Workspace

A formal security awareness training program is in place to guide personnel on maintaining appropriate security for VMware services. Access control, separation of duties and other policies define which individuals are allowed to have access to VMware Cloud Services management systems, and serve as an integrity function for unauthorized access to tenant data. Access to customer environments where the customer's data is stored requires an authorized VMware operator to authenticate via two-factor authentication to an access control system to generate a user-specific, time-based credential required for access. Generation of these temporary credentials must be tied to a specific incident. All activity performed by the users is logged. The VMware Security Operations Center uses log capture, security monitoring technologies and intrusion detection tools to look for unauthorized access attempts or any VMware personal accessing customer data. All changes to the virtual machine configuration are logged and available to the customer, which enables detection of tampering and integrity checking.

Policy

VMware has policies and procedures in place to establish and maintain a safe and secure working environment. VMware personnel as well as involved third parties receive VMware Business Conduct Guidelines and security awareness training regarding these documents' policies, standards and procedures.

Asset management

VMware maintains inventories of critical assets, including asset ownership, as well as an inventory of critical supplier relationships.

Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally owned assets are required to be returned within an established period. VMware monitors systems for privacy breaches and has a breach notification process to notify customers in the event of a privacy breach.

Governance, risk and compliance

Risk assessments, program management and policy

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 reduce the risk related to the confidentiality, integrity and availability of sensitive information.

VMware Cloud Services management has a strategic business plan that includes risk identification and the implementation of controls to mitigate or manage risks. VMware Cloud Services management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and 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.

VMware Business Conduct Guidelines and security awareness training are required upon hire and annually for employees. VMware provides security policies and security training to employees to educate them as to 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 perform reviews against industry standards, including ISO 27001. VMware will furnish audit reports under an NDA as they become available.

VMware has documented security baselines to guide personnel in ensuring 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 and baseline configurations are securely recorded. VMware notifies customers when material changes are made to the service.

Supply chain management, transparency and accountability

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 are controlled based on the principle of least privilege—only the minimum level of access required shall be granted. Access 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 ISMS program. VMware utilizes internal/external audits as a way to measure the conformance and effectiveness of the controls applied to reduce risks associated with safeguarding information and identify areas of 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 includes security provisions. Supplier agreements are in place to ensure providers are in compliance with applicable laws, security and privacy obligations. Customers are responsible for utilizing our solution in compliance with relevant laws and regulations.

VMware has a formal process to document and track non-conformance as part of our ISMS, and monitors supplier performance and escalates issues as necessary. To assure reasonable information security across your information supply chain, 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.

Sub-processing agreements are reviewed as part of the VMware audit and assessment program. VMware monitors provider audit reports and certifications to review risk management and governance processes, and effectiveness of applicable controls.

VMware has made SLAs, Terms of Service, Data Processing Addendums and Privacy notices publicly available. They can be found at *vmware.com/download/eula*.

Audit assurance and compliance

VMware engages independent third-party auditors to perform reviews against industry standards and will furnish audit reports under an NDA as they become available. For more information concerning available compliance reports and other security and compliance information, please visit *cloud.vmware.com/trust-center/compliance*.

Enterprise resilience

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 or man-made disasters. As 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 roles and responsibilities supported by regular workforce training.

VMware ensures that security mechanisms and redundancies are implemented to protect equipment from utility service outages. A risk assessment is completed on a regular basis to identify natural and man-made threats based on 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 reviewed through regular audits.

VMware facilitates the determination of the impact of any disruption to the organization through defined documents that identify all dependencies, critical products and services. The real-time status of a VMware Cloud Services offering along with past incidents is publicly available at *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 to ensure high availability of the VMware Cloud Services offering, including regional independence, and separation of console availability and customer service availability. VMware Cloud Services leverages the specific underlying Amazon Web Services 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 Amazon Web Services in the event of a failure. VMware has developed processes with Amazon Web Services to ensure that we have defined responses in place in the event that an upstream event occurs.

The architecture of Amazon Web Services provides tremendous redundancy, such that customers who run their workloads in multiple regions are effectively operating across multiple providers. However, customers who require redundancy of their workloads on another provider can use VMware HCX to replicate workloads.

As part of the VMware business impact analysis, dependencies on third parties are documented to ensure appropriate business continuity measures are in place.

Customers may report a disaster via self-service, or they may call the VMware global support team. VMware will review customer-reported events and determine if the event meets the criteria of a disaster. VMware provides a tenant-triggered failover option so workloads can be failed over per a pre-defined policy or through manual event triggering.

The VMware business continuity plans and documentation are reviewed as part of the enterprise independent attestation process annually. The VMware ISMS is based on the ISO 27001 framework. Business continuity and redundancy plans are reviewed by VMware third-party auditors that perform reviews against industry standards, including ISO 27001. VMware will furnish audit reports under an NDA as they become available.

Conclusion

The reach of security does not have to end where the public cloud begins. A cloud solution must deliver end-to-end hybrid cloud security by using common technology and operational models between the on-premises data center and the public cloud. VMware Cloud Services can help enterprises achieve this by extending trusted IT security frameworks to the cloud, embedding security policies to follow workloads anywhere and providing a holistic cloud infrastructure based on your business needs.

Supporting documentation

Terms of Service

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-cloud-services-universal-tos.pdf

Data Processing Addendum

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-data-processing-addendum.pdf

VMware Privacy Policy

https://www.vmware.com/help/privacy.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 312215aq-wp-vmcloudonaws-uslet. 8/19