Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	VMware, Inc.		DBA (doing business as):	N/A	
Contact Name:	Narayan Bharadwaj		Title:	Vice President, Products	
Telephone:	N/A		E-mail:	compliance@vmware.com	
Business Address:	3431 Hillview Ave		City:	Palo Alto	
State/Province:	CA	Country:	USA	Zip:	94304
URL:	https://cloud.vmware.com/vmc-aws				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Sebastian Schmidt		Title:	Principal Consultant	
Telephone:	303-554-6333		E-mail:	coalfiresubmission@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	Colorado	Country:	USA	Zip:	80021
URL:	https://www.coalfire.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	VMware Cloud on Amazon Web Services (VMC on AWS)	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☒ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☒ Other services (specify): Infrastructure Management	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	None	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	VMware Cloud on Amazon Web Services does not directly store, process or transmit cardholder data (CHD). As a managed Software Defined Data Center (SDDC) service provider, VMware Cloud on Amazon Web Services offers virtualization services to its customers on AWS public cloud infrastructure, which they may implement within their own cardholder data environment (CDE). Other than the telemetry data received from monitoring systems deployed in the customer's environment, VMware Cloud on Amazon Web Services does not access or interact with customer data.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	The VMware Cloud on AWS is a unified Software Defined Data Center (SDDC) platform that integrates vSphere, vSAN, and NSX on top of bare metal hardware from AWS. Customers leveraging the service have the ability to provision Software Defined Data Centers (SDDCs) and make use of the unified platform to transmit and store any kind of data, including cardholder data (PAN).

	VMware does not process or have access to customer data stored within customer SDDCs.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
AWS Hosted Data Centers	The number of facilities of this type are limited to those reflected within the most recent AOC for AWS.	Please refer to locations listed within the most recent AOC for AWS.

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	N/A	N/A	N/A	N/A

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	VMware Cloud on AWS is an Infrastructure as a Service (IaaS) offering that provides VMware managed Software Defined Data Centers (SDDCs) consisting of vSphere, vSAN, and NSX running top of bare metal hardware from AWS. Customers leveraging the service can provision SDDCs on-demand and use these environments to run virtual machines that are capable of transmitting and storing any kind of data, including cardholder data (PAN). As the service provider, VMware does not process or have access to customer data stored within SDDCs. **Shared Responsibility Model** VMware Cloud on AWS operates in a shared responsibility model where specific tasks are performed by the customer, VMware, and AWS. The shared responsibilities are as follows. Customers are responsible for “Security in the Cloud” with specific requirements to secure and manage their virtual machines, applications, and the configuration of networking and security of their SDDC. VMware is responsible for “Security of the Cloud” with specific requirements to patch and upgrade the SDDC components including vCenter Server, vSphere, vSAN and NSX Manager. AWS is responsible for “Security of the Infrastructure” with specific requirements to maintain physical security of the data centers and configuration and operation of the physical

servers, networking and security devices deployed therein.

Some key points taken into consideration by Coalfire to determine the scope and applicable PCI DSS requirements for VMware include:

- Customers are not given root access to ESX or administrator access to vCenter Server.
- Customers are given a tightly scoped administrative role in vCenter Server (cloudadmin@vmc.local) that enables management of virtual machines, datastores, and virtual networking.
- Customers are given a tightly scoped administrative role in vCenter Server (cloudadmin@vmc.local) that prevents them from performing low level SDDC configuration changes such as patching and upgrading vCenter, ESX, and NSX.
- VMware site reliability engineers (SREs) perform all low level SDDC configuration changes as part of the managed offering.
- VMware SREs perform maintenance and upgrades on customer SDDCs to the meet commitments described in our published SLA and Service Description documents.
- VMware SREs periodically perform upgrades on customer SDDCs, and there is no option for customers to "stay behind" on a release or freeze changes to their SDDC. Between a customer's inability to modify SDDC configuration and not being able to “stay behind” on an update or release, VMware is able to ensure that the entire fleet of SDDCs always remain in a last-known-good state.

VMware Cloud on AWS Site Reliability Engineering (SRE) Team

VMware Cloud on AWS is operated by a dedicated team of site reliability engineers (SREs) that have primary responsibility for the operations of the VMC Service (vmc.vmware.com) and the fleet of customer deployed SDDCs. The SRE team operates a set of operational systems that enable management of the service. The systems operated by SRE include:

- SDDC Point of Presence (PoP)
- VMware Developer Platform (VDP)
- Operator Console

	▪ Delegated Access ▪ Logging ▪ Monitoring ▪ Change Management **VMware Cloud on AWS Extended Teams** Supporting the VMware SRE team are several additional VMware teams. These teams provide specialized services and support for the offering, but do not have direct access to the VMC Service or to customer deployed SDDCs: ▪ VMware Security Operations Center (SOC) ▪ VMware Information Security (InfoSec) ▪ VMware Information Technology (IT) ▪ VMware Human Resources
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No
If Yes:	

Name of service provider:	**Description of services provided:**
Amazon Web Services	Cloud Hosting Provider
Note: *Requirement 12.8 applies to all entities in this list.*	

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed:	VMware Cloud on Amazon Web Services

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	**Requirement 1.1.3 –** N/A. VMware does not directly store, process and/or transmit cardholder data, and have no direct knowledge as it relates to SDDC customers consuming its VMC on AWS service offering. **Requirement 1.2.2 –** N/A. VMware does not maintain any routers that are in scope. **Requirement 1.3.6 –** N/A. VMware does not directly store, process and/or transmit cardholder data, and have no direct knowledge as it relates to SDDC customers consuming its VMC on AWS service offering.
Requirement 2:	☐	☒	☐	**Requirement 2.1.1 –** N/A, No wireless environment in-scope within the VMware Cloud on Amazon Web Services. **Requirement 2.2.3 –** N/A, there are no insecure services, daemons or protocols enabled. **Requirement 2.6 –** N/A, VMware Cloud on Amazon Web Services is not a shared hosting provider.
Requirement 3:	☐	☒	☐	**Requirement 3.1, 3.2, 3.3, 3.4 –** N/A. VMware does not directly store, process and/or transmit cardholder data, and have no direct knowledge as it relates to SDDC customers consuming its VMC on AWS service offering. **Requirement 3.6 –** N/A**.** VMware does not share encryption keys with its customers. **Requirement 3.6.6 –** N/A**.** VMware does not implement any manual clear-text cryptographic key-management operations.

Requirement 4:	☐	☒	☐	**Requirement 4.1, 4.1.1 –** N/A, VMware Cloud on Amazon Web Services does not transmit or receive cardholder data over open, public networks.
Requirement 5:	☐	☒	☐	**Requirement 5.1, 5.1.1, 5.2, 5.3 –** N/A, None of the in-scope system components assessed required anti-virus software.
Requirement 6:	☐	☒	☐	**Requirement 6.4.3 –** N/A, VMware does not have any instance in where PANs (live or otherwise) are used or needed for testing. **Requirement 6.4.6 –** N/A, no significant change occurred within the past 12 months within the environment.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**Requirement 8.1.5 –** N/A, VMware Cloud on Amazon Web Services does not allow any vendors to access the VMC on AWS environment remotely. **Requirement 8.5.1 –** N/A, VMware Cloud on Amazon Web Services does not have remote access to customer CDE. **Requirement 8.7 –** N/A, VMware Cloud on Amazon Web Services does not store, process or transmit cardholder data on any in-scope systems components.
Requirement 9:	☐	☒	☐	**Requirement 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1 –** N/A, VMware Cloud on Amazon Web Services does not utilize any media including removable media containing sensitive data to be moved outside the data centers. **Requirement 9.8, 9.8.1, 9.8.2 –** N/A, VMware Cloud on Amazon Web Services does not utilize any electronic media or hard-copy materials containing cardholder data to be stored in the data centers. **Requirement 9.9, 9.9.1, 9.9.2, 9.9.3 –** N/A, VMware Cloud on Amazon Web Services does not process any card-present transactions from any system including point-of-sale (POS) devices.
Requirement 10:	☐	☒	☐	**Requirement 10.2.1 –** N/A, VMware Cloud on Amazon Web Services does not store any cardholder data within the in-scope systems.
Requirement 11:	☐	☒	☐	**Requirement 11.1.1 –** N/A, No wireless environment in-scope within the VMware Cloud on Amazon Web Services environment. **Requirement 11.2.3 –** N/A, No material change to the VMware Cloud on Amazon Web Services environment occurred that would have required an unscheduled scan.
Requirement 12:	☐	☒	☐	**Requirement 12.3.9 –** N/A, VMware Cloud on Amazon Web Services does not allow third-party/vendor remote access into its applications and system components. **Requirement 12.3.10** – N/A, VMware Cloud on Amazon Web Services does not access cardholder data.

Appendix A1:	☐	☐	☒	**A1.1, A1.2, A1.3, A1.4 –** N/A, VMware Cloud on Amazon Web Services is not a shared hosting provider.
Appendix A2:	☐	☐	☒	**A2.1, A2.2, A2.3 –** N/A, VMware Cloud on Amazon Web Services does not have POS POI terminal connections.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	01/25/2021	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *01/25/2021.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *VMware, Inc.* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, *N/A* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: *N/A* An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met
N/A	N/A

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Tenable Network Security, 5049-01-09*

Part 3b. Service Provider Attestation

DocuSigned by:
Narayan
FF16C6D7E345409...

Signature of Service Provider Executive Officer ↑	*Date:* 1/25/2021 | 3:35 PM PST
Service Provider Executive Officer Name: **Narayan Bharadwaj**	*Title:* **Vice President, Products**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted PCI DSS v3.2.1 remote and onsite assessment and documented compliance results in the Report on Compliance (ROC) and the associated Attestation of Compliance (AOC).

DocuSigned by:
Sebastian Schmidt
68D696D7D036491...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 1/25/2021 | 4:34 PM MST
Duly Authorized Officer Name: **Sebastian Schmidt**	*QSA Company:* **Coalfire Systems, Inc.**

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Not Applicable.

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐