



# **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):	
Contact Name:	Vladimir Smirnov	Title:	Director of Technical Operations
Telephone:	N/A	E-mail:	compliance@vmware.com
Business Address:	3401 Hillview Avenue	City:	Palo Alto
State/Province:	CA	Country:	USA
		Zip:	94304
URL:	https://sdwan.vmware.com/		

#### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	360 Advanced, Inc.		
Lead QSA Contact Name:	Virgil Floresca	Title:	Security Architect
Telephone:	1-866-418-1708	E-mail:	vfloresca@360advanced.com
Business Address:	200 Central Ave., Suite 2100	City:	St. Petersburg
State/Province:	FL	Country:	USA
		Zip:	33701
URL:	http://www.360advanced.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:		SD-WAN Services
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services (specify):</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input checked="" type="checkbox"/> Other services (specify): SD-WAN	<b>Payment Processing:</b> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> 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: Not Applicable

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:

### Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

VMware SD-WAN does not store, process, or transmit cardholder data within the VMware SD-WAN management and data-plane networks. The transmission of customer cardholder information is limited to the system components that reside exclusively in the SD-WAN PCI environment and encrypts all traffic and data using AES- 256.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

Not Applicable

### 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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>



Amazon Web Services 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.
VMware Corporate Office	1	Palo Alto, CA, USA

**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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

**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 SD-WAN is a service offering product from VMware that provides software-defined Wide Area Network capabilities to VMware customers. The service gives customers the software abstraction to create a network overlay and decouple network software services from the underlying hardware. The transmission of customer cardholder information is limited to the system components that reside exclusively in the SD-WAN PCI environment and encrypts all traffic and data using AES- 256. As a service provider, VMware may service customers that fall into any one of the payment channels, but the customer cardholder data is never available nor made accessible to the service provider.

Does your business use network segmentation to affect the scope of your PCI DSS

Yes  No



environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*



**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: Not Applicable

QIR Individual Name: Not Applicable

Description of services provided by QIR: Not Applicable

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 services

**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:		SD-WAN Services		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>1.1.3 was not applicable. The VMware SD-WAN system components do not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management plane of the SD-WAN service. VMware is not responsible for data-flow diagrams of cardholder data and does not maintain an architecture of systems or applications within their clients’ environments.</p> <p>1.2.3 was not applicable. The VMware SD-WAN PCI environment resided solely within data centers managed by AWS, a Level 1 PCI DSS-validated service provider, who does not maintain in-scope wireless networks within the hosted environments.</p> <p>1.3.4, 1.3.6, and 1.4 were not applicable. The VMware SD-WAN system components do not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management plane of the SD-WAN service.</p>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>2.1.1 was not applicable. The VMware SD-WAN PCI environment resided solely within data centers managed by AWS, a Level 1 PCI DSS-validated service provider, who does not maintain in-scope wireless networks within the hosted environments.</p> <p>2.2.3 was not applicable. VMware did not enable insecure services, daemons, or protocols including SSL</p>





				<p>/ early TLS within the VMware SD-WAN PCI environment.</p> <p>2.6 was not applicable. VMware offers no services to PCI customers that would classify them as a shared hosting provider.</p>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>3.1, 3.2, 3.3, 3.4 – 3.4.1, 3.5 – 3.5.4, 3.6 – 3.6.8, and 3.7 were not applicable. The VMware SD-WAN service does not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management and data plane of the SD-WAN service itself. VMware supports network management for customers who may transmit CHD but does not have access to any CDE from either the management or data plane.</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>4.1 – 4.1.1, 4.2, 4.3 were not applicable. The VMware SD-WAN service does not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management and data plane of the SD-WAN service itself. VMware supports network management for customers who may transmit CHD but does not have access to any CDE from either the management or data plane.</p>
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>5.1 – 5.1.1, 5.2, and 5.3 were not applicable. The VMware SD-WAN service is comprised of system components provisioned using a hardened virtual appliance image of the Ubuntu Linux operating system. These virtual appliances were not considered to be commonly affected by malicious software.</p>
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>6.4.3 and 6.4.4 were not applicable. VMware SD-WAN is a service offering that provides Software Defined Wide Area Network (SD-WAN) management to VMware customers. VMware SD-WAN does not store, process, or transmit cardholder data. VMware supports network management for customers who may transmit CHD but there is no access to any CDE from VMware, therefore VMware's developers have no access to live PANs or any need for testing with test PANs.</p> <p>6.4.6 was not applicable. No significant changes occurred within the past 12 months. However, processes are in place to implement applicable PCI DSS requirements and update documentation as a result of any significant changes to the VMware SD-WAN PCI environment.</p>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>8.1.5 was not applicable. VMware did not have vendors who accessed system components within the VMware SD-WAN PCI environment.</p>



				<p>8.3.1 and 8.7 were not applicable. The VMware SD-WAN service does not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management and data plane of the SD-WAN service itself. VMware supports network management for customers who may transmit CHD but does not have access to any CDE from either the management or data plane.</p> <p>8.5.1 was not applicable. VMware did not require or maintain remote access to customer sites or systems.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.1.2 was not applicable. The VMware SD-WAN PCI environment resided solely within data centers managed by Amazon Web Services, a Level 1 PCI DSS-validated service provider, who did not have network jacks that were publicly available.</p> <p>9.5.1, 9.6 – 9.6.3, 9.7 – 9.7.1, and 9.8 – 9.8.2 were not applicable. 360 Advanced confirmed that the VMware SD-WAN service does not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management and data plane of the SD-WAN service itself. VMware supports network management for customers who may transmit CHD but does not have access to any CDE from either the management or data plane.</p> <p>9.9 – 9.9.3 were not applicable. VMware SD-WAN does not support or manage point of sale devices that capture payment card data via direct physical interaction.</p>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>11.2.3 was not applicable. VMware did not implement any significant changes to their environment or applications within the assessed examination period that required rescans outside of the standard quarterly schedule.</p> <p>11.3.4 – 11.3.4.1 were not applicable. Segmentation was not used to isolate the VMware SD-WAN PCI environment from other networks. This environment was hosted solely within the AWS cloud environment in which all system components were considered in-scope for this assessment.</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>12.3.9 was not applicable. VMware did not have vendors or business partners with access to the VMware SD-WAN PCI environment.</p> <p>12.3.10 was not applicable. VMware SD-WAN service does not directly store, process, or transmit cardholder data but only provides the infrastructure platform that hosts the management and data plane of the SD-WAN service itself. VMware supports network management for customers who may transmit CHD but does not have</p>



				access to any CDE from either the management or data plane.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Appendix A1 was not applicable. VMware SD-WAN offers no services to PCI customers that would classify them as a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Appendix A2 was not applicable. VMware SD-WAN does not support or manage point of sale devices that capture payment card data via direct physical interaction.

## 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:	March 24, 2021
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated March 24, 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**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>VMware</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

- |                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment. |
| <input checked="" type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Tenable, Inc.</i>   |

**Part 3b. Service Provider Attestation**

DocuSigned by:

*Vladimir Smirnov*

619AE759D2CF4B9...

Signature of Service Provider Executive Officer ↑

Date: March 31, 2021

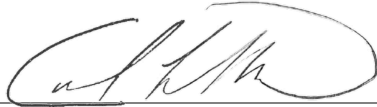
Service Provider Executive Officer Name: Vladimir Smirnov

Title: Director of Technical Operations

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

If a QSA was involved or assisted with this assessment, describe the role performed:

360 Advanced provided PCI DSS assessment and system compliance services.



Signature of Duly Authorized Officer of QSA Company ↑

Date: March 31, 2021

Duly Authorized Officer Name: Carl Lindblad

QSA Company: 360 Advanced, 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

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

