



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022



Document Changes

| Date | Version | Description |
|----------------|---------------------|--|
| September 2022 | 3.2.1 Revision 2 | Updated to reflect the inclusion of UnionPay as a Participating Payment Brand. |



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: | Wazuh Inc. | | DBA (doing business as): | N/A | |
| Contact Name: | Santiago Bassett | | Title: | CEO | |
| Telephone: | 1-408-724-0059 | | E-mail: | santiago@wazuh.com | |
| Business Address: | 1021 Lenor Way | | City: | San Jose | |
| State/Province: | CA | Country: | United States | Zip: | 95128 |
| URL: | https://wazuh.com | | | | |

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

| | | | | | |
|------------------------|-----------------------------|----------|---------------|-----------------------|-------|
| Company Name: | MegaplanIT Holdings, LLC. | | | | |
| Lead QSA Contact Name: | Mark Repka | | Title: | Security Consultant | |
| Telephone: | 1-602-761-7678 | | E-mail: | MRepka@Megaplanit.com | |
| Business Address: | 18700 N Hayden Road #340 | | City: | Scottsdale | |
| State/Province: | AZ | Country: | United States | Zip: | 85255 |
| URL: | https://www.megaplanit.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: Wazuh Cloud (Logging Aggregation System)

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):
Log Generation, Aggregation and Storage

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: N/A

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.

Wazuh provides a cloud-based platform in which agents installed on various on premises and cloud system devices for their clients, report usage statistics, logs, and vulnerability scanning of system components back to the central cloud hub.

Payment for services rendered is available on the website via Secure I-Frame to the Stripe processor. Wazuh does not receive any PAN in this process.

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

Wazuh does not directly or indirectly handle credit card data within their cloud-based logging aggregation system. It is possible for clients to leak credit card data into Wazuh systems in the logs to which they aggregate. The log aggregation system is not purposed for storage, transmission, or processing of credit card data.

Wazuh does not store, process, nor transmit cardholder data with their cloud based log aggregation system. Payments for the cloud service may be made through their website via secure I-Frame to Stripe.

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> |
| Cloud Hosting Provider | 1 | AWS, USA |
| Cloud Hosting Provider | 1 | London, UK |
| Cloud Hosting Provider | 1 | Frankfurt, GE |
| Cloud Hosting Provider | 1 | Singapore, HK |
| Cloud Hosting Provider | 1 | Sydney, AUS |

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) |
|--------------------------|----------------|--------------------|---|--|
| N/A | N/A | N/A | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | N/A |
| | | | <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.*

The assessor observed connections in and out of the Wazuh Cloud environment, data-flows from Wazuh agents, firewalls, access control mechanisms, and system settings. In addition, the assessor observed trial, retail, development, and administrative environments for the Wazuh Cloud services.

Wazuh does not store, process, nor transmit cardholder data with their cloud based log aggregation system. Services rendered may be paid on a Wazuh website via secure I-Frame integration with Stripe Inc.

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

Wazuh instances are hosted in AWS cloud hosting solution. The cloud hosting solution contains all instances of administration, clients, test, and development environments. The instances for different clients are all separated and each client has their own instance of Wazuh running. There is no multiple tenancy within the environment.

Stripe Inc.

Payment Processor

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: | | Wazuh Cloud (Logging Aggregation System) | | |
|---------------------------|----------------------------------|--|--------------------------|---|
| PCI DSS Requirement | Details of Requirements Assessed | | | Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.) |
| | Full | Partial | None | |
| Requirement 1: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 1.1.6- Entity does not employ insecure protocols, ports, or services. 1.2.3- Entity does not employ wireless networking. 1.3.6- Entity does not store cardholder data. |
| Requirement 2: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 2.1.1- Entity does not employ wireless networking within the production environment. 2.2.3- Entity does not employ any insecure services, protocols, or daemons. 2.6- Entity is not a shared hosting provider. |
| Requirement 3: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 3.1.c- Entity does not store cardholder data. 3.2- Entity does not receive any SAD. 3.3- Entity does not host any form of PAN data. 3.4.a-3.4.c- Entity does not store PAN anywhere in the environment. 3.4.1- Entity does not employ full disk encryption. 3.5-3.6- Entity does not host PAN in any form, no key management required. |
| Requirement 4: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 4.1- Entity does not host or transmit any cardholder data. 4.1.1- Entity does not employ wireless networking in the production environment. |



| | | | | |
|-----------------|-------------------------------------|-------------------------------------|--------------------------|---|
| Requirement 5: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 6: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 6.4.6- No significant changes have been made to the environment within the last 12 months. |
| Requirement 7: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 8: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 8.1.5- Entity does not allow third-party access to the environment. 8.6- Entity does not employ "Other" authentication mechanisms. 8.7- Entity does not host any databases containing cardholder data. |
| Requirement 9: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 9.5-9.8.2- Entity does not host any physical media with cardholder data. 9.9- Entity does not host any devices for the capture of cardholder data. |
| Requirement 10: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Requirement 11: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 11.2.3- Entity has not had significant changes that have required additional scanning. 11.3.4- Segmentation is not employed in the environment. |
| Requirement 12: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A1: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | N/A- Entity is not a shared hosting provider. |
| Appendix A2: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | N/A- Entity does not host POI terminals. |



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: | 12/13/2023 |
| 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 **12/13/2023**.

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>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Wazuh, Inc.</i> has demonstrated full compliance with the PCI DSS.</p> | | | | | | |
|-------------------------------------|--|----------------------|--|--|--|--|--|
| <input type="checkbox"/> | <p>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, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date 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>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">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, Version 3.2.1 r2</i> , 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 ¹ , CAV2, CVC2, CVN2, CVV2, or CID data ² , or PIN data ³ 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>SAINT</i> |

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑

Date: 20/12/2023

Service Provider Executive Officer Name: **Santiago Bassett**

Title: **CEO**

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

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

The assessor conducted a full level 1 PCI DSS audit including review of documents, data-flow diagrams, network diagrams, personnel interviews, and data collection.

DocuSigned by:

Mark Repka

FC3884B918B4498...

Signature of Duly Authorized Officer of QSA Company ↑

Date: 12/26/2023

Duly Authorized Officer Name: Mark Repka

QSA Company: MegaplanIT Holdings, LLC.

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:

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

