SERVICE DESCRIPTION

Managed Security and Compliance (MSC) - Compliance Essentials

Trustwave Managed Compliance Security Services for Hospitality and Retail

Through packaged bundles designed specifically for the demands of the hospitality industry, we make easy for you to address PCI compliance and security without disrupting your focus. Whether you need basic validation services or full network security management with connectivity services, we deliver security the way you want it.

Compliance Essentials Package Summary

With our Compliance Essentials Package, we can help you simplify compliance with the PCI DSS and provide the tools you need to assess, track and document your compliance status. In short, we take the hassle out of meeting the basic PCI Validation and management requirements, so you can focus on your business.

Package Feature	What you get
Vulnerability Scanning	Detect and address vulnerabilities in your environment with quarterly external vulnerability scans to address PCI requirements and provide critical information regarding potential network security concerns.
Self-Assessment Questionnaire (SAQ)	Simplify the process of your SAQ, through our PCI Wizard, automated To-Do List, and free professional guidance.
Information Security Policy	Establish security best practices for your business with the help of our information security policy template.
PCI Training	Fully educate your employees with our PCI training module that includes customized training courses, course exams and training completion certificates.
Cloud-based Portal Access	Gain complete visibility to your network and validation services through our single, centralized and cloud-based customer portal TrustKeeper.

Customer Support	Get valueable assistance when you need it, with 8x5 support for your business and your compliance programs.
Breach Protection	Get financial peace-of-mind with $50,000 in breach coverage for your business.

Note: The Compliance Essentials Package does provide template support for completing a SAQ-D. It does not provide course completion tracking / reporting and content customization.

External Vulnerability Scanning

As an Approved Scanning Vendor, Trustwave performs certified quarterly external vulnerability scans to help address PCI requirements and provide critical information regarding potential network security concerns. If required to perform scanning of card-processing environment, the Trustwave proprietary scanning engine becomes an integral component of your compliance process. The activities and Client/Trustwave responsibilities are within the External Vulnerability Scanning service description and are not specified in this service description.

The EVS service consists of:

- Discovery, which is the information gathering and discovery process to understand the Client's System Target(s) and the scope of the required scanning of those targets.
- Scanning helps to identify potential vulnerabilities or weak configurations of the Clients System Target(s).
- Reporting is the provision of results of the Client Target System(s) scans, as a completed report available through the TrustKeeper Client Portal.

Base Features

Basic service features overview

The EVS service includes the following basic service features:

TrustKeeper Client Portal access providing:

- Tracking of provisioning progress
- EVS portal account subscription
- Client Target System entry
- Change management and support requests creation and response
- Reporting

Discovery

During this phase the Client information is collected, and a port scan of the Client's network is completed.

Scanning

Unlimited self-service scans during the EVS Scan Period, based on the predefined Scan Profile selected by the Client is performed on the Client's Target System(s).

Reporting

Predefined reports are available through the TrustKeeper Client Portal, including PCI DSS reports for compliance.

Self-Assessment Questionnaire (SAQ)

Trustwave provides a PCI SAQ Wizard in the TrustKeeper Portal to simplify the process of filling out the correct SAQ for submission to the Card processor. Assistance with correctly filling in the questionnaire is available through SOC support analysts. The SAQ is a required document for completion of the PCI submission and compliance requirements.

Information Security Policy

Establish security best practices for your business with the help of our information security policy template. Having a security policy in place is a requirement of PCI. The Trustwave information security policy template allows the Client to have a framework that they can use to incorporate the security policy information that is unique to their environment.

Security Awareness and PCI Compliance Training

Trustwave provides PCI education for employees on credit card security procedures with PCI training module in the TrustKeeper Portal. Having a security training program is a requirement for PCI compliance. The security awareness training is provided through the Trustkeeper Portal making the availability and tracking of the delivery of the training material easy for Clients to help achieve compliance with this PCI requirement.

TrustKeeper Client Portal

The TrustKeeper Client Portal provides the Client with access to the expertise of the SOC staff, security information and analysis and the Trustwave Platform. The available features and functionality of the TrustKeeper Client Portal set out below may differ depending on the relevant Trustwave managed security service acquired by the Client.

The TrustKeeper Client Portal includes the following:

- Designated Client contact information;
- Track progress of the service rollout;
- Provides a method for the Client to securely communicate with the Trustwave MSS provisioning and SOC personnel;
- Access device configuration and status information;
- Security software (such as the TrustKeeper Agent) if applicable to the relevant Trustwave service;
- Upload documentation and security policies;
- View security data and other security related data providing a current security posture of the Clients environment to the extent possible with services provided by Trustwave;
- Review current security events and Security Alerts of Client's Trustwave-monitored network(s), as well as historical data;
- Review and track status of Client change requests to equipment installed on Client's premises or within the Client's environment; and
- Create and track support tickets.

Payment Card Breach Protection

Trustwave, through its insurance broker and carrier, has obtained the option for breach protection that can provide operators with up to $50,000 or $100,000 per merchant ID to cover expenses resulting from a payment

card compromise. These costs may include fees for forensics investigations, payment card re-issuance, punitive fines from the card brands, ADCR (“fraud”) expenses and other mandatory expenses imposed by the card brands.

Trustwave is not an insurance broker or carrier and is not selling insurance to Client or their remote operators. Rather, Trustwave will procure an insurance policy from an insurance carrier through a licensed insurance broker that will provide insurance coverage as “Additional Locations” under the Trustwave policy to Client’s who are identified by Client for Trustwave services and pay the related services fees hereunder. The insurance policy specifically relates to data compromises that occurred due to a security incident as defined in the insurance policy and Client customer will be provided coverage when, and only when an accurate MID is provided to and accepted by the third-party insurance carrier. Insurance coverage is only effective during the month or months that the accurate MIDs are provided to and accepted by the Insurance Carrier. Trustwave is not responsible for, nor will it assume any responsibly or liability whatsoever for verifying the accuracy of any MIDS provided by either Client or their franchisees. Trustwave does not make and specifically disclaims any and all representations or warranties regarding the insurance policy and Client agrees to look only toward the insurance policy and the carrier for resolution of any associated claims. Client shall indemnify Trustwave for any claims related to non-coverage as a result of an inaccurate or omitted MID.

Trustwave, in its sole discretion, has the right to cancel, terminate, replace or modify the terms of the Trustwave obtained insurance policy or the terms and conditions of obtaining coverage under the policy at any time and without notice. Furthermore, Trustwave shall have the right to replace, supplement, or other change the third-party insurance broker and carrier at any time in its sole discretion. Trustwave or the third-party insurance carrier or broker shall publish a copy of the then-existing insurance policy via the internet for merchant review along with claims processing information. Client and its franchisees agree that any and all coverage shall be subject to the terms of the applicable insurance policy.