Trustwave Service Description

Trustwave Endpoint Protection Suite

Contents

Trustwave Endpoint Protection Suite

SERVICE DESCRIPTION

Trustwave Endpoint Protection Suite is a powerful, cloud-based security solution that delivers integrated anti-malware, policy enforcement and simplified compliance management. By integrating core endpoint protection functions, Trustwave simplifies management and lowers security operational costs for greater adoption and optimal defense-in-depth against a wide range of threats. Modules for rogue device detection, file integrity monitoring and log collection further enhance your security.

Trustwave Endpoint Protection Suite Summary

Package Feature	What you get
Cloud-based Portal Access	The Trustwave cloud-based delivery model reduces hardware costs and management overhead, allowing easier coverage of diverse and distributed endpoints, including laptops, tablets, and mobile and fixed point-of-sale (POS) systems.
Client Support	Get valuable assistance when you need it, with 8x5 support for your business and your compliance programs.
Security Health Check & Security Configuration	Unifies your endpoint protection to provide maximum visibility and control for your entire organization to help ensure PCI standards are met and to deliver powerful and comprehensive endpoint security. Verifies endpoint security settings are configured in a secure manner and that proper security policies are configured for items, such as user password management, system configuration, system auditing and system logging. Quickly check scan results at-a-glance with the TrustKeeper cloud portal.
Credit Card Data Scanner (DLP)	Endpoints with prohibited and unencrypted credit card data pose a great risk of exposure. Reduce the risk exposure of data loss, potential fines and remediation costs with a tool that helps ensure your endpoints are free of unencrypted credit card data. Scans your endpoints for unencrypted credit card data, including card number/PAN and credit card track data with a high level of accuracy.

Unauthorized Device Monitor	Rogue devices are weak links that provide attackers with an easy target to breach your network. Help ensure only authorized devices are on your network with quick and easy detection of rogue devices that may present a risk of breach, such as unauthorized wireless access points, personal devices (smartphone, laptop, etc.) and retired equipment that should not be connected. Scans the network and identifies all connected endpoint devices to help verify that no unauthorized devices are connected.
IP Beacon	Provides peace of mind and critical protection to help ensure that Client's endpoints are consistently and automatically scanned without manual IP tracking or updating – even those with dynamic and frequently changing external IP addresses. Consistently collects and sends endpoint external IP addresses for inclusion in the Trustwave Vulnerability Management profile.
File Integrity Monitoring (FIM)	FIM helps Clients to more easily meet relevant PCI DSS requirements and rapidly detect malware with consistent reporting on file changes, including those made by malware, unauthorized users and Windows updates. Monitors endpoints for changes to critical system objects, such as file directories and registry settings, and provides the important details you require for analysis through the TrustKeeper cloud portal.
Trustwave AV	Delivers powerful, real-time protection with the simplicity that comes from cloud delivery, which eliminates the need for on-site management servers. Provides real-time protection against threats on the endpoint, downloaded from the internet and even threats on remote or removable drives, such as USB thumb drives. Scans endpoints for dormant threats waiting to be activated. Signature updates are provided in real-time as available, sometimes occurring multiple times an hour.
Mobile Security	Delivers powerful, on-demand protection for mobile devices with the simplicity that comes from cloud delivery, which eliminates the need for any on-site management servers.

	Trustwave Mobile Security extends endpoint protection to mobile devices with modules that protect against insecure configuration, malware threats, network-based attacks, privacy attacks and data leakage from installed applications, and secure two-factor authentication to protect social media and other online accounts.
Windows Log Collection	Provides a simple and easy method for collecting and centrally storing required endpoint logs for your compliance and other security audits. Collects endpoint logs, including Windows event logs, plain text files, and syslog messages from devices that are compatible with Trustwave Managed SIEM. Logs are collected into an internal queue, filters are applied and then the file is sent via the TrustKeeper cloud to Trustwave SIEM for event correlation, alerting and reporting.

TRUSTWAVE ENDPOINT PROTECTION SUITE FEATURE DESCRIPTIONS

File Integrity Monitoring (FIM)

Trustwave's FIM service is a solution that monitors additions, modifications, or deletions of sensitive files or other stored data by performing periodic checks and displaying the data for Client through the TrustKeeper portal when a file modification is detected.

FIM Deployment

Trustwave's FIM service can be deployed on POS devices, laptops, desktops and servers as a module on the Trustwave Endpoint Protection Platform to all Microsoft Windows and Linux OS versions currently supported by endpoint protection. Trustwave FIM reports changes to the following object types:

- Files
- Directories
- Registry keys
- Registry values

The FIM service is delivered in the cloud via Trustwave's TrustKeeper portal. All detected changes are collected and delivered to the Trustwave Endpoint Protection backend and visible through the TrustKeeper portal FIM view. Trustwave will maintain one year of FIM event data available for forensic review upon request, after which the data will be purged. This FIM event data can optionally be forwarded to the MSS SOC for additional analysis if Client is also subscribed to a compatible MSS SIEM service, in accordance with the terms of the SIEM service agreement.

Trustwave FIM deploys as a software module on the Trustwave Endpoint Protection Suite (EPS) platform for both Microsoft Windows and Linux OS platforms. The service can be added to an existing EPS implementation and installed on each supported endpoint automatically. If Client has not deployed the EPS, the client software is installed when the FIM service is deployed.

FIM Template Support

Trustwave will leverage pre-configured templates to enable monitoring of critical system configurations. Client is responsible for specifying any additional objects beyond the supplied template.
As a general guideline, a custom FIM template can be developed for any application, on a time and materials basis, if all of the following criteria are met:

- Request for FIM template is delivered in writing or via TrustKeeper portal support ticket
- Application is deployed on a supported EPS OS
- Application stores its critical configuration and file objects on the endpoint filesystem or in the Windows registry (registry only supported on Windows OS)
- Client makes available to Trustwave's engineers (preferably by remote access) an existing deployment of the application in its environment that is the same as production
- There are no differences in the endpoint used to build the template and the endpoint that is to be monitored
- Client is responsible for all travel expenses for on-site work necessary to build the FIM templates
- Client understands that custom FIM templates do not support change severity detection

A separate statement of work, or contract addendum, is required for any custom FIM template work. A custom FIM template project is billed on a per-project, time and materials basis.

FIM Event Management

Once Trustwave's FIM service has been deployed to all applicable devices, the monitoring aspect of the service is considered live. Client is responsible for reviewing events from Trustwave FIM through the TrustKeeper portal. Individual FIM events include details of the specific machine, file modified, and time stamp.

Security Health Check & Security Configuration

This feature helps ensure Client's desktop endpoint settings are configured in a secure manner and that proper security policies are in place to provide maximum visibility and control for your entire organization to help meet PCI requirements and deliver powerful protection. This feature also performs a series of health audits on mobile POS devices to proactively protect and defend your fleet.

Windows Log Collection

Offers a simplified method for collecting and centrally storing required endpoint logs for your compliance and security audits, and works with Trustwave SIEM to provide event correlation, alerting and reporting. Once Trustwave's logging service has been deployed to all applicable devices, the monitoring aspect of the service is considered live. All logs are collected and Client reviews log events in the Trustwave MSS portal.

The EPS-LOG-COLLECTION SKU must be included in the quote in order to use EPS for Windows Log Collection along with the appropriate MSS SIEM SKUs.

Credit Card Data Scanner (DLP)

Fixed endpoints with prohibited and unencrypted credit card data pose a great risk. Helps eliminate the exposure of data loss, potential fines and remediation costs with the critical assurance that your endpoints are free of unencrypted credit card data.

Unauthorized Device Monitor

Rogue devices are weak links that provide attackers with an easy target to breach your network. This monitor helps ensure only authorized devices are on your network with quick and easy detection of rogue devices that may present a risk of breach, such as unauthorized wireless access points, personal devices and retired equipment.

IP Beacon

Synchronizes dynamic IP address information with TrustKeeper for automated scanning of mobile and fixed endpoints. Available on Windows, macOS, Linux, and Android.

Trustwave AV

Real-time malware protection. Provides real-time protection against threats on the endpoint, remote or removable drives and threats downloaded from the internet – and scans for dormant threats waiting to be activated to protect your organization against advanced targeted attacks. New Endpoint Protection Suite customers can download an installer from the TrustKeeper portal. Existing Endpoint Protection Suite customers can request that Trustwave AV be manually pushed to existing endpoints. Real-time protection is only available on the Windows platform and is not available on Linux or Android. Trustwave AV on Linux provides daily and on-demand scanning of the device for malware threats. Automatic malware threat quarantining is only available on the Windows and Linux platforms.

Virus Definition Updates: Trustwave will provide anti-virus definitions in realtime via CDN. These updates by default are automatic but can be configured to be delivered on an hourly, daily, or manual basis.

Endpoint Reporting: All Trustwave AV data can be reviewed in the TrustKeeper AV application. In addition, data can be viewed locally on machines where Trustwave AV is installed.

Trustwave AV Deployment

Trustwave's AV service can be deployed on POS devices, laptops, desktops, and servers as a module of the endpoint protection suite to all Microsoft Windows, macOS, and Linux versions currently supported by the Endpoint Protection Suite.

The AV service is delivered in the cloud via Trustwave's TrustKeeper portal. All detected malware threats are quarantined, reported to the TrustKeeper backend, and visible through the TrustKeeper portal AV view. The backend will forward these events to the MSS SOC for additional analysis and alerting. Trustwave will maintain 30 days of AV update history, the most recent plus seven days of full scan data, and all data available online in the TrustKeeper portal AV view. Trustwave will also maintain all AV event data for forensic review for up to one year upon Client request.

Trustwave AV deploys as a software module on the Trustwave Endpoint Protection Suite (EPS) platform. The service can be added to an existing EPS implementation. If Client has not deployed the EPS, the software is installed when the AV service is deployed.

EPS will aggregate and securely relay the AV event data to Trustwave's SOC for processing and analysis. In the event of a network disruption, the EPS application buffers the data until such time as connectivity has been restored.

Trustwave will provide all maintenance of the EPS software as a part of the Trustwave Managed AV service. Updates to the standard AV template are included.

The AV event data is transmitted from Client's site to Trustwave facilities where the data is automatically normalized, aggregated, correlated and scored.

MOBILE SECURITY

Trustwave Endpoint Protection Suite

Trustwave Endpoint Protection Suite is a powerful, cloud-based security solution that delivers integrated anti-malware, policy enforcement and simplified compliance management. By integrating core endpoint protection functions, Trustwave's solution simplifies management and lowers security operational costs for greater adoption and optimal defense-in-depth against a wide range of threats. Trustwave Mobile Security extends this protection to mobile devices with modules that help protect against insecure configuration, malware threats, network based attacks, privacy attacks and data leakage from installed applications, and secure two-factor authentication to protect social media and other online accounts.

Trustwave Endpoint Protection Suite – Mobile Security Summary

Package Feature	What you get
Client Support	Get valuable assistance when you need it, with 8x5 support for your business and your compliance programs.
Mobile AV	Delivers powerful, on-demand protection for mobile devices using the Android operating system with the simplicity that comes from cloud delivery, which eliminates the need for on-site management servers. Provides automatic, on-demand, and daily scan protection against threats on the device, installed via USB, and downloaded from the internet. Scans devices for dormant threats waiting to be activated. All applications are scanned immediately after installation and/or update. Signature updates are delivered live in the cloud during online scanning.
Device Configuration Scanner	Verifies that the security policy and settings of the device are configured in a secure manner. Users are presented with a list of settings which may need to be corrected. On

	Android, the user may request that the settings be updated automatically in most cases. Instructions are provided to help the user correct any issues discovered.
Privacy Scanner	Scans all installed applications to determine what permissions have been granted to each application. Mobile Security then categorizes these permissions and presents them to the user. The user can review and choose to uninstall any application if they so desire.
WiFi Network Scanner	Scans the WiFi network that the device is connected to. Warns user when they connect to an in-secure or unencrypted WiFi network. Actively tests the connected WiFi network for common attacks. When malicious behavior is detected, the user is warned to disconnect from the network, and the malicious behavior is reported to the Trustwave WiFi hotspot reputation scoring service. Provides a reputation score for each WiFi hotspot.
Two-Factor Authentication	Help protect your online financial, social media, shopping, and other accounts from unauthorized access with two-factor authentication. Supports Time-based One Time Password (TOTP) code generation using the open standard based on RFC 6238. This feature is supported by many popular online services and financial institutions.

MOBILE SECURITY - FEATURE DESCRIPTIONS

Mobile AV

Anti-Virus and Anti-Malware protection for the Android platform. Provides daily-scan and on-demand protection against threats on the endpoint, remote or removable drives and threats downloaded from the internet – and scans for dormant threats waiting to be activated to protect your devices against advanced targeted attacks. Provides automatic, daily, and on-demand scanning of the device for malware threats. Automatic scanning is completed for every application after it is installed or updated. Because mobile AV uses cloud-based signature verification during scans, online access is required for malware scans and updates are made in real-time. Signatures are not stored on device for offline use.

Mobile AV is only available on the Android OS for devices using ARM and x86 processors.

Device Configuration Scanner

Scans devices to verify that the device is configured securely. Users are presented a screen that shows which settings have passed or failed the scan. The user may select each item, read more information about what passed or failed, and get help for correcting any failures. On Android, many of the settings can be corrected for the user by tapping the “Fix This For Me” button. For settings that can be

automatically fixed, the user is given either a web link for more information, or Mobile Security will walk the user through correcting the failure with on-screen help. The device configuration scanner detects changes as soon as they are made.

For iOS devices, some of these settings require enrollment in Trustwave's TrustKeeper Cloud iOS MDM solution. If the user opts not to enroll in MDM, results for these settings will be unavailable and marked accordingly.

Privacy Scanner

Scans all installed applications to determine what permissions have been granted to each application. Mobile Security then categorizes these permissions and presents them to the user. The user can then review and uninstall any application if they so desire.

WiFi Network Scanner

Scans the WiFi network that the device is connected to. Warns user when they connect to an in-secure or unencrypted WiFi network. Actively tests the connected WiFi network for common attacks, including:

- SSL tampering
- DNS tampering
- Captive portals
- HTTPS link stripping
- Content tampering/ad injection
- Other Man-In-The-Middle attacks

When malicious behavior is detected, the user is warned to disconnect from the network with an OS notification. Malicious behavior is also reported to Trustwave's WiFi hotspot reputation scoring service. Trustwave uses the malicious behavior reports to create a 1-5 aggregate reputation score for each WiFi hotspot that can be used to help determine whether a network is risky even when malicious behavior is not currently detected.

Two-Factor Authentication

Helps protect online financial, social media, shopping, and other accounts from unauthorized access with two-factor authentication. Supports Time-based One Time Password (TOTP) code generation using the open standard based on RFC 6238. This feature is supported by many popular online services and financial institutions. Users can add new accounts manually or by scanning a QR code provided by the service provider. RFC 6238 relies on a shared secret that is stored on the device and at the service provider. This does not require any special integration between Mobile Security and the service provider.

Mobile Security Application Delivery

Mobile Security for Android devices is delivered through the Google Play store using an account owned and operated by Trustwave. The Google Play Store URL for Mobile Security is:
https://play.google.com/browse.php?com.trustwave.mobile

Mobile Security for iOS devices is delivered through the iTunes App Store using an account owned and operated by Trustwave. The iTunes App Store URL for Mobile Security is:
https://itunes.apple.com/us/app/trustwave-mobile-security/id1186053206?mt=8

Trustwave Mobile Security may not be distributed by Client using any means other than the app store URL listings in this document without prior written approval by Trustwave.