SERVICE DESCRIPTION

Firewall and Technology Management

Overview

In Trustwave's Firewall and Technology Management service ("**Service**"), Trustwave will manage and maintain Client's third-party security technology or technologies indicated in the applicable SOW or Order Form according to its system design ("**Managed Technology**"). The Service supports either on-premises and cloud native types of Managed Technology. The following description sets out the parameters of the Service.

Service Variations

The Service is available in different variations according to the type of Managed Technology (each a "**Service Variation**"). Client's applicable Order Form or SOW will indicate if any and which Service Variation is included. Trustwave may support network security Managed Technology devices of three types: intrusion detection prevention systems (IDPS), next generation firewall (NGFW), and secure access service edge (SASE). However, Trustwave will only support certain features for each such device type (see table below). The "X" indicates which features are included in the Service for each device type.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Feature Description*	IDPS	NGFW	SASE
Threat Prevention Threat prevention features search for known viruses, spyware, and worms. Depending on the vendor, additional capabilities of this feature may include drive-by protection and behavioural-botnet detection.	X	X	
Sandbox Analysis Sandbox analysis is a static and dynamic analysis over multiple operating systems and application versions. This feature analyzes samples of files and links and tags items for further investigation. Automatic quarantine can occur when categorization is malicious.	X	X	
Security Policy Management A firewall policy which allows for add/change/remove based on requested criteria or inputs from threat intelligence.		X	X
URL Filtering URL filtering allows for control of access to internal resources by granting or denying access to resources based on predetermined criteria and threat intelligence databases.		X	
Web Content Filtering Web content filtering uses web content classification to prevent users from accessing known malicious sites or inappropriate content.		X	
VPN VPNs are encrypted communication links between supported devices for a site-to-site VPN or enablement of remote users to a supported device.		X	
Secure Remote / Private Access Provides secure user access to private enterprise apps and resources.			X
Cloud Access Security Broker (CASB) CASB serves as a gateway to cloud services, provides visibility of cloud activities, threat and data protection, enforcement of security policy, and ease of compliance with regulatory policies.			X
Secure Web Gateway (SWG) SWG is internet and URL filtering software that provides an inline proxy between users and the internet that enables prohibited content blocking and threat prevention for cloud and web traffic.			X

*This is a description of the feature for identification purposes. Trustwave does not guarantee this is how the feature will function.

Core Features

The Service includes the following core features:

Trustwave Fusion Platform & Fusion Mobile App

The Trustwave Fusion platform is Trustwave's proprietary cloud-based security operations platform. Client and Trustwave will cooperate to add the Managed Technology to one Client account in the Trustwave Fusion platform as part of the Onboarding feature (see below). Client will have access to the following capabilities and related documentation on the Trustwave Fusion platform via web or mobile application:

- Security Event information, Fusion Alerts, and Security Incidents (each as defined below)
- Device health and availability tickets
- Client's reports and dashboards
- Request methods for change support and management
- Methods of communication including tickets and chats
- Such capabilities are available to Client in the Trustwave Fusion platform, including allowing for
- Ticketing integration

Client is responsible for any further connectivity, access, health, and advanced ticketing integrations between Client infrastructure, software, the Managed Technology, and the Trustwave Fusion platform. Any changes to connectivity, services, and documentation for the Trustwave Fusion platform advanced integrations are at Trustwave's sole discretion.

Log Ingestion

The Service includes only the ingestion of system logs. The Service does not alone include security monitoring of any ingested logs. No events data will be collected, analyzed, and responded to. Trustwave will not ingest more than two hundred thousand (200,000) system logs per day. Where Client has purchased Threat Monitoring and the Service, Trustwave will classify **Security Events** based on EDR and SIEM data from the Managed Technology integrated into the Trustwave Fusion platform and they will be treated as raw logs with no expectation of threat detection outcomes.

Connectivity

Client and Trustwave will work together to connect the Trustwave Fusion platform and the Managed Technology using one or more of the following connection methods (subject to the applicable SOW or Order Form between Client and Trustwave).

- **Trustwave Connect**: A virtual appliance jump box hosted in Client's environment that allows Trustwave to remotely connect the Trustwave Fusion platform to the Managed Technology. Trustwave will deploy Trustwave Connect based on the model of the Managed Technology indicated in the applicable SOW or Order Form.

- **Direct Connectivity**: A direct connection between the Managed Technology and the Trustwave Fusion platform using either:
    - Trustwave-hosted managed console;
    - Client-hosted managed console; or
    - API connection to the Trustwave Fusion platform (available only with cloud-based Managed Technology via API)

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Additional Information

Where Trustwave Connect is used, Trustwave will provide Client the applicable Trustwave Connect deployment model and the necessary perimeter network access configurations for the Service.

Where a Client-hosted managed console is used to connect the Managed Technology to the Trustwave Fusion platform, Client is responsible for implementation and creating Trustwave-user accounts as requested by Trustwave. This connection method is only available to the extent explicitly agreed to by Trustwave in the applicable SOW or Order Form. Client acknowledges certain access methods may require increases in the applicable Fees.

Onboarding

Onboarding includes two components: Client-side implementation and MSS Transition.

Client-side Implementation

Client will take the necessary steps to connect Client's systems which generate Security Events to the Trustwave Fusion platform and the Managed Technology (including endpoints to management stations and sensor agents on each endpoint in scope) as agreed between Trustwave and Client in the applicable SOW or Order Form. Client will ensure the Managed Technology is prepared to provide appropriate and consistent information about Client's environment in a manner that allows Trustwave to provide the Service. Trustwave may assist Client during this phase.

If necessary for the Managed Technology to work with the Service, Client will create access groups and individual Trustwave-users in the Client environment that allow such users to deliver services. Client is responsible for providing initial and ongoing Trustwave user and system remote access to the Managed Technology to accommodate Trustwave's remote system management and threat analysis and investigation.

Trustwave will provide Client with an initial list of users during Onboarding. After Onboarding (during Steady State as defined below), Trustwave will provide Client with ongoing user access, update requests, and use change management tickets to maintain updated user access to the Client's Managed Technology. Client agrees to abide by the Change Management section and must use the Trustwave Fusion platform to document user updates. If Client fails to perform changes and maintain Client-side implementation responsibilities for Trustwave user access to Managed Technology, then Trustwave has no responsibility for providing the Service and Trustwave will not continue with this feature of the Service until Trustwave has the necessary access to the Managed Technology.

MSS Transition

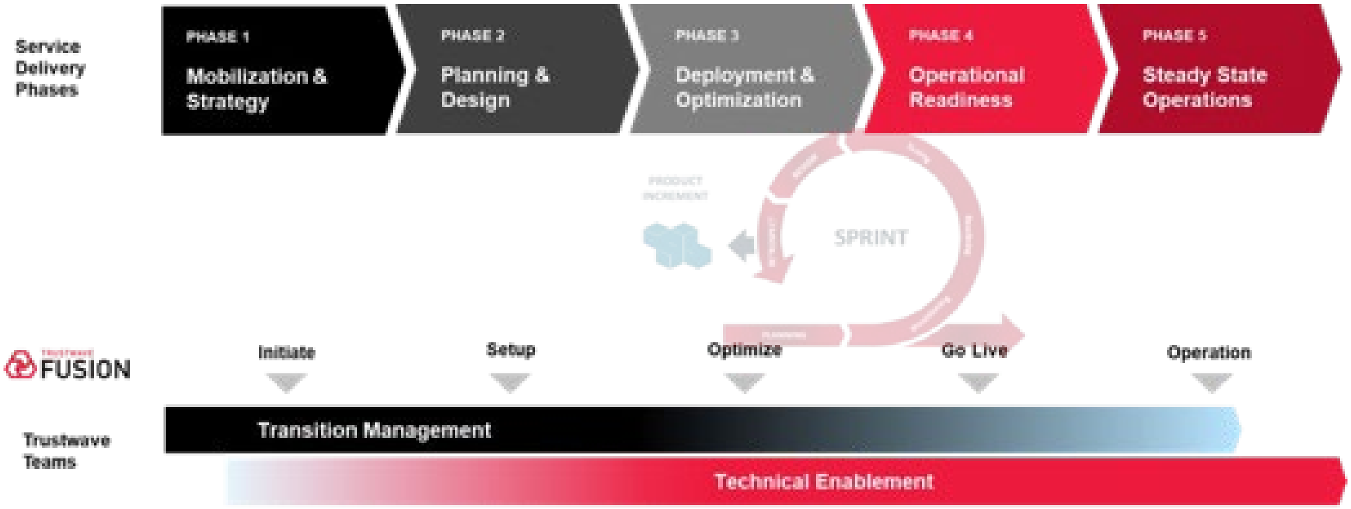
MSS Transition is designed to facilitate the integration of the Managed Technology with the Trustwave Fusion platform. Trustwave will assign a transition manager and additional technical enablement resources (at Trustwave's discretion) to work with Client on onboarding the Service. Trustwave will advise Client through five (5) phases of transition management. Client is deemed fully transitioned and

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

at steady-state (beginning of the Service features other than Onboarding) following Trustwave’s conclusion of the fifth (5th) phase (“**Steady State**”).

Transition Management Phases

The following chart summarizes the five (5) phases of transition management in this feature:



Client Obligations

For Trustwave to provide Onboarding, Client will:

- be responsible for deploying the software necessary for Trustwave to provide the Service for the Managed Technology or related telemetry;
- configure initial and ongoing network connectivity from Client systems to Managed Technology utilizing the Trustwave address ranges and domains that allow Trustwave to provide the Service;
- upon Trustwave’s request, confirm to Trustwave that Client systems are reporting to the Managed Technology in order to support log and alert collection;
- ensure Managed Technology has appropriate licensing and support contracts with third parties during the Term.

Trustwave Obligations

As a part of Onboarding, Trustwave will:

- schedule and host a kick-off meeting with Client;
- provide new-user orientation materials and training regarding the Service;
- keep Client informed of transition progress.

Service Features

The Service is offered for both on-premises and cloud native types of Managed Technology. On-premises, also known as on-prem, refers to a Managed Technology that is installed and runs on Client’s physical hardware and infrastructure. Cloud native refers to a Managed Technology delivered as a service by a third-party vendor remotely over the Internet. The following Service features apply to each type of Managed Technology according to the following table below.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Service Feature	On-Premises	Cloud Native
Systems Management	X	X
Change Management	X	X
Product and Security Updates	X	
Health and Availability Monitoring	X	
Backup and restore	X	
High Availability	X	

The Service includes the following service features:

Systems Management

Trustwave will manage and monitor the security configuration of those Client security solutions which are included in the Service as indicated in the applicable SOW or Order Form ("**Managed Security Application**") according to the following sections. For the avoidance of doubt, Trustwave will not provide the Service for any Client security solution other than what is specifically set forth in the SOW or Order Form unless otherwise agreed between Client and Trustwave in writing.

Change Management

Trustwave will administer changes to the Managed Technology based on either (i) Client-initiated changes, (ii) Trustwave-initiated changes, or (iii) according to the co-managed access model.

All change requests are classified according to the following table:

Change Request Type	Description
Emergency Change	A change which Trustwave views as necessary to mitigate immediate and material security risk(s) identified by Trustwave or Client (and communicated to Trustwave); provided that such request involves only security policy settings and is not a major software patch update for the Managed Technology.
Standard Change	Repetitive, typically low risk changes. It has repeatable implementation steps and predictable outcomes.
Complex Change	A change which meets the following criteria: • may cause technical system impact and could have significant outage effects or affects multiple business units or environments • may impact security controls • does not have repeatable implementation steps

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Project	A change which meets the following criteria: • due to its scope of work, cannot be considered as standard or complex change and specifications require Trustwave to consult Client • due to its volume, cannot be completed within SLAs agreed for Emergency, Standard, or Complex Changes • Trustwave determines such a change may alter the architectural design of the Managed Technology • may require proof of concept to be completed before executing *Note*: Projects may require Client to agree to additional services and Fees to complete this request. Classifying a change as a Project Change is at Trustwave's sole discretion.

Security Policy and Change Management

Client and Trustwave will collaborate on the initial configuration of security policies and settings for the Managed Security Application and work together during the Term to maintain that configuration. This must be completed to achieve Steady State (defined below).

When the Managed Security Application has no existing security policies, Trustwave will assist the Client in developing and applying a base policy.

Trustwave may modify these security policies and settings further at any time during the Term with the aim of protecting against threats to Client.

Client-Initiated Change Management

Trustwave will assess and implement change requests submitted by Client through Trustwave approved communication methods. Trustwave evaluates such requests against industry best practices and the change's potential cybersecurity impact on Client's security environment. Trustwave will propose a schedule and notify Client of changes Trustwave expects (in its sole discretion) may disrupt Client's environment, and Client will approve or deny these scheduled change windows. Client acknowledges that denying a scheduled change window may impact Trustwave's ability to provide the Service and service level agreements (SLAs) may not apply until Trustwave is able to implement the change

Trustwave will also notify Client if a change request is (i) so significant in scope that it would require a separate engagement between Trustwave and Client or (ii) outside the scope of the Service and, therefore, will only be performed at Trustwave's discretion.

Client acknowledges that any configuration change management requests for Managed Security Application or Client environment that are categorized as a complex change may, in Trustwave's sole discretion, be deemed a project and would require a written addendum between the Parties.

Trustwave-Initiated Change Management

Trustwave will implement Trustwave-initiated changes through the Trustwave Fusion platform. Trustwave determines the applicability of such changes against industry best practices and the change's potential impact on Client's environment. Client may review each proposed change.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Trustwave will perform the change according to the change window schedule agreed between Client and Trustwave.

Trustwave-Initiated Maintenance and Endpoint Management

Trustwave will, at its discretion, recommend version updates for the Managed Security Application. The Client will be responsible for implementing such updates and understands failure to implement may result in Trustwave's inability to provide the Service.

Trustwave will monitor the health and availability of the alert and event data from Managed Security Application that is connected to the Fusion platform. For on-premises applications, the alert and event data ingestion will be monitored via Trustwave Connect. The health and availability of the on-premises appliance(s), whether virtual or physical, and endpoints that connect to the Managed Security Application that are not directly to the Trustwave Fusion platform, are Client's sole responsibility to manage and monitor.

Co-Managed Access Change Management

Trustwave maintains access to the Managed Security Application and may provide Client with access permissions to the Managed Security Application if Client requires co-management of the Managed Security Application's feature sets. Such additional access permissions may include:

- **Read Only**: Default option. Trustwave fully manages the Managed Security Application. Client can monitor Managed Security Application, but not directly alter without contacting Trustwave.
- **Role Based**: Co-managed option (as permitted by Trustwave). Trustwave grants Client partial access to manage the Managed Security Application. See below for related restrictions.
- **Full Admin**: Co-managed option (as permitted by Trustwave). Trustwave grants Client full access to manage the Managed Security Application. See below for related restrictions.

If granted Role Based or Full Admin access permissions, Client agrees to the following shared change and change audit process:

- <u>Restrictions</u>: Before implementing any changes to the Managed Security Application, Client will create a change ticket in the Trustwave Fusion platform, identifying which policies and configuration settings will change and of any other planned effects. Upon receiving the ticket, Trustwave may review changes made by Client and make recommendations.
- Client acknowledges this co-managed structure may result in increased risk of security incidents or Service outages. Client will work in good faith with Trustwave to remediate any such security incident and perform a root cause analysis. If Trustwave reasonably determines that the security incident or outage was caused by a change or activity performed by Client, Client will be solely responsible for the effects of the change and for completing and producing the root cause analysis. Additional charges for co-managed access may apply and will be included on the SOW or Order Form.
- Client representatives with co-managed access to the Managed Security Application will be responsible for attaining reasonable competency and training in cybersecurity to make standard changes to the Managed Security Application's rules and configurations. Client is responsible for validating such competency and training.
- Client will address all Trustwave-initiated changes for access in a timely manner that allows Trustwave to maintain access and compliance with prescribed Service terms. Failure to respond to these requests will negatively impact the response time outlined in the Service description.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Client Obligations

For Trustwave to provide this feature of the Service, Client will:

- procure and maintain valid vendor software licenses and maintenance contracts applicable to the for Client owned Managed Security Application;
- monitor and maintain patches, health, and connectivity of Client's non-Trustwave managed systems, software, and EDR agents to any Managed Security Application, including security application on-premises appliance(s) and networking equipment and applications.
- provide, when requested by Trustwave, prompt access to third-party vendor portals to allow for software and license downloads and provide necessary authorizations for Trustwave to act on behalf of the Client for management and maintenance purposes;
- access the Trustwave Fusion platform to submit change ticket requests, respond to tickets, and confirm scheduled change windows;
- consider risk factors related to change requests and promptly provide requested information to Trustwave;
- review and assess changes that Trustwave proposes and promptly provide Trustwave with approval or rejection of such proposals;
- at Trustwave's reasonable request, provide pre-determined change control windows during which change management functions can be executed;
- inform Trustwave of all maintenance activities and changes in Client's environment that may impact Trustwave's ability to provide the Service; and
- provide Trustwave with access to the Managed Security Application.
- ensure the Managed Technology can be supported or maintained by its vendor or manufacturer for a minimum 9 months before end of life (EOL). To be supported or maintained the managed technology would still be receiving security updates, bug fixes and other forms of support for a minimum period of at least 9 months from the vendor or manufacturer.

Trustwave Obligations

For this feature and upon Client reaching Steady State (see Onboarding feature below), Trustwave will

- provide Service-related remote assistance, support, and configuration within the Managed Technology and Managed Security Application. For the avoidance of doubt assistance for on-premise appliances will be limited to the Managed Security Application software operating on the appliance;
- attempt to resolve connectivity or application issues identified regarding the Managed Security Application to return it to a steady state of operation. Assistance for on-premises appliances will be provided after the Client has provided sufficient evidence of no existing environmental issues or self-initiated changes to the infrastructure that may negatively impact the steady-state operation of the appliance;
- perform assessment of a change request based on Trustwave's risk level and change categories and determine whether a change request is in-scope for the Service;
- Trustwave may notify Client if a change request is outside the scope of the Service or if additional charges will apply to a change request;
- perform change management activities only in compliance with Trustwave policies;
- Trustwave may audit any Client-directed change and confirm whether there are any errors or consequences resulting from the change. If Trustwave determines no additional action is required, Trustwave may close the relevant change ticket. If Trustwave's review raises any

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

questions or concerns, Trustwave may communicate such questions or concerns to Client and Client will work with Trustwave to resolution.

- Trustwave will not be responsible for the design, implementation, effect, or any damages, direct or indirect, of any Client changes made to the Managed Security Application, Managed Technology, or Client-managed systems the Service relies upon.
- provide product and security update recommendations and assistance with issues resulting from upgrades;
- source additional information as necessary to support the implementation of the change request;

Product and Security Updates

Trustwave may apply security updates, product updates, and patches to the Managed Technology. Trustwave will recommend such updates or patches to Client via the Trustwave Fusion platform. Client will approve or deny such recommendations within twenty-four (24) hours of the Trustwave Fusion platform notification. Client agrees that its refusal of or failure to reply to such Trustwave recommendations will suspend Trustwave's obligations under any agreed SLAs for that Managed Technology. Client further agrees that if its configuration of the Managed Technology prevents Trustwave from implementing security updates, product updates, and patches, this may adversely impact the operation and functionality of the Managed Technology, the Service, or any applicable Trustwave service.

Update types relevant to this Service feature include:

- **Security Content Updates**: Typically, new content for protection engines (initiated by the vendor of such protection engines) to address the latest threats. Client will ensure the Managed Technology is configured to automatically download Security Content Updates and if not, Trustwave will not be responsible for implementing such updates.

- **Patches or Hotfixes**: Updates to address immediate and specific product issues initiated by the vendor for such products.

- **Product Features Updates**: Updates to address feature issues provided by the vendor of the applicable product. These updates will typically cause brief downtime or restart of the Managed Technology. Application of product feature updates requires a pre-defined change control window that Trustwave will coordinate with Client. Trustwave will assess such updates on a case-by-case basis to determine whether the update is a Standard Change or a Complex Change.

- **Indicators of Compromise (IOCs) Updates**: Updates done either at Client's specific request, automatically based on IOC packages delivered by the Managed Technology vendor (performed by the vendor, Trustwave is not responsible for such updates), or based on Trustwave's research for EDR products. IOCs are artifacts observed on a network or in an operations system likely to be indicating a computer intrusion.

Trustwave will (i) monitor the availability of security updates, product updates, and patches and (ii) apply such updates to the Managed Technology at Trustwave's discretion, which may be subject to (but is not limited to) the following:

- Updates or security patches that include bug and vulnerability fixes will be reviewed by Trustwave and applied to the Managed Technology only when the update applies to any active subscriptions or feature set.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

- Subject to Client ensuring Trustwave has all required access rights granted, Trustwave will schedule product and security updates available under the relevant Managed Technology license or support and maintenance contract with Client prior to implementation.
- Trustwave may accommodate Client's preferred maintenance window to minimize disruptions. Trustwave will implement the relevant product and security updates according to its assessment of priority.
- Trustwave will only be responsible for implementing updates from the Managed Technology vendor operating system (OS) and is not responsible for updates to the hardware OS hosting the Managed Technology.
- If available from the Managed Technology's vendor, Trustwave may perform an immediate emergency patch upgrade or workaround on the Managed Technology. Trustwave will notify Client of the completed Emergency Change.

For updates and patches which constitute Emergency Changes initiated by Trustwave and are related to critical vulnerabilities (critical vulnerabilities are security weaknesses or flaws in the Managed Technology that could be exploited by attackers to compromise the integrity, confidentiality, or availability and are deemed of a critical nature by Trustwave), Trustwave reserves the right to apply updates or patches if Client does not review and approve or deny the submitted Trustwave-initiated update or patch within twenty-four (24) hours of the initial notification. Trustwave is not liable for any consequences for Client's failure to respond to such notifications.

Health Status Monitoring

For on-premises Managed Technology, the Service includes limited health and availability monitoring. Where Trustwave has identified health or availability issues with the Managed Technology, Trustwave may triage and remediate such issues (if appropriate and at Trustwave's discretion). If Trustwave takes remediation steps and they are not successful, Trustwave will notify and may work with the Client on the issue via a ticket in the Trustwave Fusion platform.

Health monitoring metrics supported by Trustwave will vary according to the Managed Technology included in the Service. Health monitoring metrics may include, but are not limited to:

- **Network Availability**: Determines if the Managed Technology shows as available via the network interface
- **CPU Utilization**: Provides measurement of CPU utilization and warns of overutilized CPU that could threaten the Managed Technology's functions
- **Disk Space**: Provides advanced warning of full disk/volume/filesystem utilization
- **Heat Indicators (device temperature)**: Alerts Client if the Managed Technology reaches defined threshold temperature (only applies to physical appliances and not for VM implementations)
- **Component Connectivity**: Monitors system components for their uptime activity, their connections, their availability of data
- **Data Management**: Monitors for license quota or queue thresholds and abnormal thresholds of data flow (low data, high data)
- **System Errors**: Tracks logs and errors of system functions to monitor stability of the Managed Technology.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.

Backup and Restore

Trustwave, at its sole discretion, will back up the Managed Technology configuration and policy to save the latest version of the configuration. Any such backups are kept for ninety (90) days from initial back up action.

High Availability (HA) Management

If HA Management is included in the Service (as indicated in the Order Form or SOW), Trustwave will:

- synchronize changes to the Managed Technology with any of its in-scope HA configurations; and
- monitor an HA Managed Technology to determine if it is online and operating normally;

Ticket Handling

Communications on the above Service features between Trustwave and Client are handled via tickets in the Trustwave Fusion platform. Trustwave typically processes tickets according to Information Technology Infrastructure Library (ITIL) standards. Trustwave will triage and troubleshoot Client's tickets.

Client Obligations

Client will

- Provide accurate and detailed information about the issue or request that becomes a ticket, including system information, error messages, and any steps taken to resolve it already;
- Ensure Client has access or privileges to make a request in the Trustwave Fusion platform; and
- Respond promptly to any requests for additional information or clarification about the issue or request from Trustwave.

Trustwave Obligations

- Trustwave will confirm receipt of properly submitted tickets in the Trustwave Fusion platform and may provide updates on the progress of the ticket.
- Trustwave will assign the ticket to the appropriate team and prioritize according to the severity of the issue and its potential impact.

Problem Management

A problem is a cause or potential cause of one or more incidents impacting the health of the Service. Client agrees to report problems through the Trustwave Fusion platform. Client and Trustwave agree to collaborate on problem resolution subject to Trustwave policy.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable Statement of Work or Order Form between Trustwave and Client.

Copyright © 2024 Trustwave Holdings, Inc. All rights reserved.