TESSIAN

TESSIAN PRODUCTS SPECIFICATION

This Products Specification should be read in conjunction with the Tessian Terms and Conditions.

SPECIFICATION

Tessian offers four Modules: (i) the Tessian Platform, (ii) Tessian Guardian, (iii) Tessian Enforcer and (iv) Tessian Defender.

The successful operation of the processes described below is subject to a successful connection being established between the Tessian Server and the Local Software.

For the purposes of this Products Specification:

"API" means the connection created between Tessian and Customer's email primary email server for the purposes of Customer providing Customer Data to Tessian

"Add In" means the .MSI file comprising the add-in for the Microsoft Outlook email client used by Customer, to be installed either locally onto each Device or into Customer's remote environment in accordance with the Agreement.

"Administrators" means an employee of Customer who has been granted administrative privileges in respect of the Services by Customer.

"**Default Threshold Period**" means 3 seconds for the Add-in and 15 seconds for the Gateway.

"Gateway" means the email gateway which emails will be routed through and will be configured by setting up a connector or routing agent on Customer's primary email server

"Local Software" means the Add-In software, API software, together with any other software provided or made available from time to time by Tessian to Customer for installation by Customer in accordance with this Agreement within its own local or remote environments.

"**Sender**" means an Authorized Mailbox's user who gives an instruction to Customer's email system to send an email (e.g. by pressing the 'Send' button)

"Tessian Server" the Tessian hosted data processing components of the overall Tessian solution.

<u>Tessian Architect</u>

Tessian Architect allows Administrators to implement customizable rules which will specify: (i) criteria to identify certain categories of emails; and (ii) the action which will be taken in respect of any email which meets the specified criteria (e.g. "blocking and auditing any email that is being sent to an external domain containing an .XLSX attachment") ("**Customized Rule**").

If a Sender issues an instruction to Customer's email system to send an email, the following process applies when the Tessian Platform is in use:

1. The Tessian Server is called by the Add-in or Gateway.
2. The Tessian Server determines whether the email meets the criteria specified in the Customized Rule.
3. If the email meets the criteria in the Customized Rule, the Tessian Server will relay a message back to the Add-in or Gateway, which will then perform the specific action of the Customized Rule (e.g. generate an audit log, display a warning notification, block the email from being sent, etc.).

If the Add-in or Gateway cannot connect to the Tessian Server or do not receive a response from the Tessian Server within the Default Threshold Period, the outgoing email will be sent to the recipient without any warning notification being presented to the Sender or any audit log being created.

Tessian Guardian

If a Sender issues an instruction to Customer's email system to send an email, the following process applies when Tessian Guardian is in use:

1. The Tessian Server is called by the Add-in or Gateway.
2. The Tessian Server seeks to detect anomalies which may infer that the email may be sent to an incorrect recipient (e.g. where an email has been inadvertently addressed to the wrong person).
3. If anomalies detected by the Tessian Server imply that the email is being sent to an incorrect recipient, the Tessian Server will generate a warning notification or email which will be presented to the Sender. The warning message will highlight the anomalies detected and give the Sender the option of sending the email or stopping the email from being sent.

If the Add-in or Gateway cannot connect to the Tessian Server or do not receive a response from the Tessian Server within the Default Threshold Period, the outgoing email will be sent to the recipient without any warning notification being presented to the Sender or any audit log being created.

Tessian Guardian uses machine learning to detect anomalies in emails being sent. The email attributes which Tessian Guardian identifies as anomalies are constantly evolving based on learning from previous emails which have been sent or stopped from being sent. As a result, not all warning notifications generated by Tessian Guardian will accurately indicate an incorrect recipient and the Tessian Server will not generate a warning notification or an audit log for all emails sent to an incorrect recipient or an unauthorized recipient.

Tessian Enforcer

If a Sender issues an instruction to Customer's email system to send an email, the following process applies when Tessian Enforcer is in use:

1. The Tessian Server is called by the Add-in or Gateway.
2. The Tessian Server seeks to detect anomalies which may infer that the email may be sent to an unauthorized recipient.

3. If the anomalies detected by the Tessian Server imply that an email is being sent to an unauthorized recipient and the email meets the criteria in the Customized Rule, the Tessian Server will permit one of the following actions to take place:

   (a) The email will be sent to the recipient and the Tessian Server will generate an audit log which may be viewed by an Administrator but no warning notification will be presented to the Sender.
   (b) The Tessian Server will send a warning notification to the Sender and give the Sender the option to proceed with sending the email or to stop the email from being sent.
   (c) The Tessian Server will send a block notification to the Sender and the email will not be sent to the recipient.

If the Add-in or Gateway cannot connect to the Tessian Server or do not receive a response from the Tessian Server within the Default Threshold Period, the outgoing email will be sent to the recipient without any warning notification being presented to the Sender or any audit log being created.

Tessian Enforcer uses machine learning to detect anomalies in emails being sent. The email attributes which Tessian Enforcer identifies as anomalies are constantly evolving based on learning from users' sending behaviors. As a result, not all warning emails detected by Tessian Enforcer will be being sent to unauthorized recipients.

<u>Tessian Defender</u>

If an Authorized Mailbox's user issues an instruction to Customer's email system to send an email or receives an email, the following process will apply when Tessian Defender is in use:

1. The Tessian Server is called by the Add-in or Gateway.
2. The Tessian Server seeks to detect anomalies which may infer that the email may have been received from a suspicious sender.
3. If anomalies detected by the Tessian Server imply that the email has been received from a suspicious sender, the Tessian Server will generate a warning notification which will be presented to the Sender explaining the anomaly.

Tessian Defender uses machine learning to detect anomalies in emails being received. Due to the predictive nature of the system, not all suspicious emails will be identified as such by Tessian Defender.

IMPORTANT NOTE: Customers using Google GSuite with Comprehensive Mail Storage enabled should note that because of the way Google configures this service, Tessian Defender will not work and should not be used or relied on.

<u>Historical Report</u>

A Historical Report is a report of malicious inbound email (for Tessian Defender), data exfiltration attempts (for Tessian Enforcer) and misaddressed emails (for Tessian Guardian) that the Customer has experienced in the past based on the analysis of the Customer's historical email data (please note that we are unable to analyse email attachments in a Historical Report).

In order for Tessian to produce the Historical Report, Customer will need to grant permission in their relevant Office 365 admin consoles or their Outlook add-in (for customers using exchange on-premise) or Google

Workspace API (used for Google customers) for Tessian to view the user mailboxes identified by the Customer to Tessian and to view their user mailboxes and to view their directory of the Customer's users. Tessian will upload copies of the emails contained within the relevant inboxes, extract the relevant metadata required for analysis (**Analysed Data**) and then create the Historical Report from its analysis of the Analysed Data (Tessian does not store copies of the original emails). Customer may remove the access permissions at any time, although if such permissions are removed before the Historical Report is delivered then Tessian may not be able to produce the Historical Report.

The Historical Report will include an analysis of the threats that the Tessian Services would have identified and prevented with respect to the e-mails analysed, namely, data exfiltration, accidental data loss, and/or malicious emails and in the case of Tessian Enforcer, unusual patterns of user activity ("Threat Intelligence Data"). When available, the Historical Report will also utilise the Tessian Human Layer Risk Hub to provide a per user risk scoring assessment based on the Threat Intelligence Data per user.

The Historical Report is for information only. It relies on previous typical patterns and behaviours and does not reflect all email data or all recent or emerging patterns and behaviours. It is intended for use as an aid to the Customer in making an informed judgment.

Audit Logs

The Tessian Server creates audit logs of key events from the Tessian Platform, Tessian Guardian and Tessian Enforcer. Administrators may request a record of audit logs in a .CSV file format via the Tessian Server. In addition, Administrators may request a daily email notification from the Tessian Server giving them a snapshot of elements of the audit log data from the past 24-hour period.