Trustwave®
Smart security on demand

trustwave.com

Terms and Conditions for Trustwave's "Zero Malware Guarantee" for Managed Anti-Malware Service

Trustwave's Managed Anti-Malware Service technology powered by Trustwave Secure Web Gateway is able to stop new, dynamic malware that other solutions overlook. Trustwave guarantees to detect and stop 100% of all malware propagated over the web which is capable of being scanned by the Managed Anti-Malware Service. If your systems become infected by one or more instances of malware in any calendar quarter, as confirmed by Trustwave pursuant to the procedures below, you will receive a one month extension of the term of your Managed Anti-Malware Service subscription.

1. Trustwave warrants that, during the time that you are receiving Managed Anti-Malware services, you will not be infected by malware.
   a. Malware is defined as any client side exploit which is triggered during web browsing, including exploits of vulnerabilities in popular browsers and 3rd party browser plug-ins. This includes the most popular plugins such as Adobe Flash, Adobe Acrobat Reader and Oracle Java. For embedded content such as Java, PDF and Flash, the malware definition includes the page that has embedded the content. Client side exploits don't include categories such as XSS, CSRF and other server side vulnerabilities.
   b. An infection is defined as a user browsing (via Managed Anti-Malware Service) to a web site that hosts an exploit which installs malware on that user's machine. Infection does not cover the case where the user is deliberately engaged in security testing of Managed Anti-Malware Service or where the user was involved with crafting the malware or any deliberate self-infection.
2. All infections from the same exploit or source will be handled as one claim (even if from different malware).
3. All infections of the same malware will be handled as one claim (even if from different exploits or sources).
4. This warranty only applies to Managed Anti-Malware Service powered by Secure Web Gateway version 11.5.2 and higher that is updated with the latest security updates and hotfixes at the time of infection.
5. Your Managed Anti-Malware Service must meet or exceed all of the requirements of the "Minimum Security Policy" section below at the time of the infection in order for this warranty to be applicable.
6. You are limited to one (1) warranty claim per calendar quarter. Warranty claims must be made in accordance with the "Making a Warranty Claim" section below. If you make a claim that is not validated by Trustwave, you may make another claim during the same calendar quarter but will be required to pay for Trustwave's reasonable costs and expenses that are necessary to investigate the claim.
7. This warranty does not apply to malware from password-protected or encrypted files.
8. The remedy to any breaches of this warranty is one free additional month of Managed Anti-Malware Service as set forth herein. This remedy shall be the sole and exclusive remedy in contract, tort or otherwise in respect of any infection of your systems by malware passed through the Managed Anti-Malware Service.

Making a Warranty Claim

1. You must inform Trustwave as soon as the warranty claim arises (and in any event no later than thirty (30) days thereafter) by calling +1.866.659.9097 (+1.312.267.3201) Option 2 or emailing mss@trustwave.com
2. When submitting the claim, you will need to provide the following to Trustwave:
   - A sample file of the malware
     - In the case of embedded content (Java, PDF, Flash, Silverlight), the embedding page must also be provided.
   - The original infection URL(s) (up to 10 URLs for each claim), and the date they were browsed. If the URL is no longer malicious at the time of investigation, the claim will be determined to be invalid.
   - Any other relevant information as reasonably requested by Trustwave
3. Trustwave will analyze the malware sample and the URLs that you provide. Trustwave will also review your Managed Anti-Malware Service audit log to determine which policy was in place at the time of the incident.
4. Based on the findings and using its reasonable judgment, Trustwave will make the final determination of whether you are entitled to the compensation (based on the Terms and Conditions set forth above). Trustwave will use its reasonable efforts to communicate its decision to you no later than thirty (30) days from the date that Trustwave receives all of the required information for the claim.
5. If your claim is validated and approved, you will receive a new license key for your additional free month of service.

Minimum Security Policy

The minimum policy requirements for a valid warranty claim are as follows:

- The following Secure Web Gateway policy rules must be enabled and set to block content (numbering is according to the Trustwave Default Policy as defined in Secure Web Gateway version 11.5):
  - Rule 6 – Block Customer-Defined and Trustwave Recommended Site Categories
    - Required configuration: all items under the “security” group enabled.
  - Rule 4 – Block Trojan Communication Based on Malicious Traffic
  - Rule 8 – Block Malicious Content (Malware Entrapment Engine).
    - Required configuration: (a) slider set to medium, and (b) Enable external resources pre- fetching.
  - Rule 9 – Block Malformed Binary Format Vulnerabilities
    - Required configuration: slider set to medium
  - Rule 10 – Block Malicious ActiveX, Java Applets and Executables
    - Required configuration: the condition element (named Binary Behavior Profile) configured with its default settings: all java related checkboxes enabled
  - Rule 15 – Block Spoofed Content
    - Required configuration: Enhanced Security checkbox enabled
  - Rule 20 – Block Binary Objects with invalid Digital Certificate
- Antivirus must be turned on.
- HTTPS scanning must be enabled. If disabled, Managed Anti-Malware Service cannot inspect HTTPS traffic (i.e., traffic encrypted with SSL).
- Exception lists – a customer can request specific URLs (or URL patterns) or content types to be excluded from processing and scanning by the Managed Anti-Malware Service Secure Web Gateway (SWG) engines. If a warranty claim involves a URL or content type that was excluded, then the claim is not valid, since the content will not have been scanned by the Managed Anti-Malware Service SWG engines.
  - List of policy rules that allow exclusions of content:
    - Rule 2 – Allow Trusted Sites. This rule contains a customer defined list named “Customer Defined Bypass List” which excludes the specified URLs from being scanned.
    - Rule 6 – Allow Selected ActiveX, Java Applets and Executables. A customer can request any instance of ActiveX, Java or Executable to be excluded from scanning.
    - Customer defined certificates. A customer can request certificates to be trusted by Managed Anti-Malware Service. This will impact rule 20 where any content signed by untrusted certificates will be blocked.
    - Any other rule that is defined to “Allow” certain URLs/content types.