Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Web Isolation

This Privacy Transparency Notice describes how Web Isolation ("Product") collects and processes Personal Data. Its purpose is to provide You (our current or prospective "Customer") the information You need to assess the Personal Data processing that is involved in using the Product.

1. Product Description

Symantec Web Isolation is a new solution for threat protection and prevention, without the need for detection. Web isolation is a remote browsing solution that prevents any browser-based attacks, such as malware, ransomware, and APTs (advanced persistent threats) from infecting endpoints without the need to block access to URLs and web content. By executing and rendering web pages away from users' devices, Symantec Web Isolation prevents any malicious code or content from reaching endpoints and eliminates the risk of infection (patient zero). It can be used to selectively isolate content web traffic, such as risky or uncategorized URLs for all users, where risk of browsing the public Internet is high, or to provide full isolation (isolate all web traffic) for privileged and high value users, such as executives, HR, finance, legal, etc. Symantec Web Isolation broadens web access for enterprise users, while reducing operational overhead and administration of internet usage.

Further information about the Product is available at:

https://www.symantec.com/products/web-isolation

For complete administration and overview of Web Isolation, please go to the following location: https://support.symantec.com/en_US/article.DOC10658.html

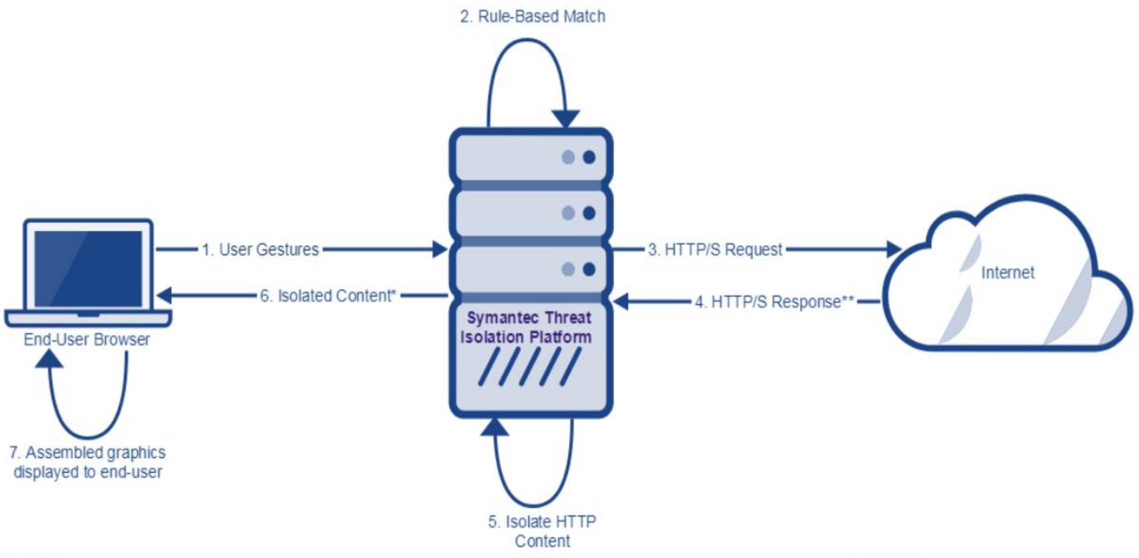
2. Personal Data Collection And Processing

Sources of Data

The following steps illustrated on the chart below describe the flow of data through the Symantec Threat Isolation Platform:

1. Each end user's gestures (i.e., mouse clicks, key presses, and changes made to the address bar) are captured in the end user's browser. This output is captured and transmitted to the Symantec Threat Isolation Platform by web-socket commands to ensure that only legitimate transactions, initiated by real end users, are performed.
2. The Symantec Threat Isolation Platform translates the end user gestures, and runs the rule-based policy on them.
3. After the rule-base decisions have been determined, when necessary, the Symantec Threat Isolation Platform generates the HTTP/S requests and transmits them to the website.
4. The Symantec Threat Isolation Platform receives the HTTP/S responses. For each element in the webpage, the Symantec Threat Isolation Platform performs a rule-based check against the organization's security policy to determine whether or not to allow the element's isolation and transmission to the end user.
5. If allowed, the Symantec Threat Isolation Platform isolates each element as a separate graphic.

6. The Symantec Threat Isolation Platform transmits the graphics to the end user's browser using a proprietary Symantec Threat Isolation protocol.
7. The end user's browser assembles all the graphics in their correct locations in the webpage canvas, and displays the isolated webpage to the end user. The Symantec Threat Isolation Platform also returns updated information for subsequent end user requests or whenever webpage data changes.



* **NOTE:**
Isolated content is secure and does not contain the original HTTP/S response

** **NOTE:**
The HTTP/S response is unsecured content that may contain malware

The Symantec Threat Isolation Platform will log each action in its network/session log if enabled, including source IP, username, browser/application, destination IP, website URL.

Respective Roles of Symantec and Customer

With respect to Personal Data transmitted from the Customer to Symantec for the purposes of the Product, the Customer is the Controller, and Your Symantec contracting entity as specified in Your applicable Agreement (“Symantec”) acts as a Processor. The rights and obligations of both parties with respect to Personal Data processing are defined in the applicable Data Processing Addendum available on the Symantec Privacy - GDPR Portal.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Online identifiers and trackers Examples: IP addresses, MAC addresses, Host/user names, Passwords and similar tokens, Device IDs and similar unique identifiers, Cookies and other user and device trackers, Individual product settings and preferences	Customer employees and contractors Other entities interacting with customer	The product utilizes Source/Destination, HTTP Request, URI/URL Information, it is collected and processed by the product to provide the administrator with access logs to review web browsing activity.
Network activity data Examples: Browsing activity	Customer employees and contractors	For isolating web browsing sessions for threat protection

and history, Telemetry, Proxy, Usage, Session logs, Traffic data, Electronic communications metadata	Other entities interacting with customer	
Network Administration of Appliance	Customer employees and contractors	Administration of appliance supportability data, it can be optionally configured to be sent to SYMC.

The Product does not need and is not meant to collect or process any Special Categories of Personal Data.

Personal Data Retention Schedule

For the duration of the contractual relationship with the Customer, Personal Data is retained as described in the applicable product description. After the expiry or termination of the contractual relationship, Personal Data is decommissioned except where its retention is required by applicable law, in which case Personal Data covered by such requirement will be further retained for the legally prescribed period.

3. Disclosure and International Transfer of Personal Data

Recipients of Personal Data

Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and external recipients (third party sub-processors), in the facilitation or provision of the Product. The list of Symantec affiliated entities and their geographical locations are available on the Symantec Privacy - GDPR Portal.

Third-Party Sub-Processors

The third-party sub-processors involved in delivering the Product are:

Sub-Processor	Personal Data	Purpose of processing	Locations
Amazon Web Services (AWS)	Contact Information	Contact end user by email and phone	US, EMEA, APAC
	Admin username and password.	Egress IP to allow to connect to the service	US, EMEA, APAC

This list is subject to change. Any planned change will be announced in advance on the Symantec Privacy - GDPR Portal. Customers can exercise their rights with respect to such changes according to the provisions of the applicable Data Processing Addendum.

International Transfers of Personal Data

You are advised that Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, including to external recipients, on the basis of European Commission Decision C(2010)593 on Standard Contractual Clauses (processors), or of any alternate, legally permitted means.

4. Exercise Of Data Subject Rights

Management of Personal Data is the responsibility of the administrator of the Symantec Threat Isolation Platform. The process for deletion and removal of personal information stored and processed in logs can be performed by resetting the activity logs.

For a complete system reset, the administrator can re-initialize the Symantec Threat Isolation Platform as follows:

Initializing the Symantec Threat Isolation Platform

1. Log in to the gateway machine console.
2. Run the following command: sudo fgcli setup
   The Network Configuration Wizard starts.
3. Follow the instructions of the wizard to perform Initial Setup.
4. The system reinitializes, and the following message is displayed: Done

Further, pursuant to the applicable Data Processing Addendum, and to the extent possible taking into account the nature of the processing, Symantec will assist the Customer, insofar as this is feasible, with the fulfillment of the Customer's obligation to respond to requests for exercising Data Subjects' rights such as the rights of access, rectification, deletion and objection laid down in Chapter III of the EU General Data Protection Regulation (GDPR).

5. Information Security

Technical and Organizational Measures

Symantec Threat Isolation can be configured to define additional administrators with full audit logging. It is Symantec's and all of its affiliated entities' commitment to implement, and contractually require all sub-processors to implement, appropriate technical and organizational measures to ensure an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of Data Subjects. Additional security documentation is available on the Symantec Customer Trust Portal.

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Product. It supersedes any prior Symantec communication or documentation relating thereto.