Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Content Analysis

This Privacy Transparency Notice describes how Content Analysis ("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 involved in using the Product.

1. Product Description

Content Analysis together with the ProxySG* or Symantec Messaging Gateway* blocks known threats, sources and signatures and centrally analyzes unknown content. Zero-day threats are automatically escalated and brokered to Symantec Malware Analysis for dynamic sandboxing and validation before sending content to users. Content Analysis is a sophisticated, multi-layer inspection platform that combines reputation services, whitelisting and blacklisting, dual anti-malware signature inspection engines, static code file analysis and on-box sandboxing to protect against known and unknown threats. Integration with Symantec Endpoint Protection* Manager and many other third-party security technologies enables threat validation, inoculation and swift remediation.

Further information about the Product is available at:

https://www.symantec.com/products/atp-content-malware-analysis

2. Personal Data Collection And Processing

Sources of Data

Content Analysis collects data from a submitting device. The list of submitters includes ProxySG*, Advanced Secure Gateway (ASG), Secure Mail Gateway*, Security Analytics* or Advanced Threat Protection*. These submitting systems will submit a file to be scanned either over Internet Content Adaptation Protocol (ICAP) or application programming interface (API) along with optional meta data about the file and or connection. Optional metadata includes, but is not limited to Client IP address of host, IP of submitting device, URL, username and time stamp.

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
Individual identifiers (names) and contact information (email, phone, address)	Customer employees and contractors	Licensing control, account setup, reporting
Location data, network activity data, communications data submitted by customer	Customer employees and contractors	Technical support

Online identifiers and trackers (IP addresses, usernames, traffic data, session logs)	Customer employees and contractors, other individuals interacting with the customer's environment	Enriched customer reporting, including on the sources of threats detected

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

Personal Data Retention Schedule

By default, data is archived 30 days, and deleted two years after the case it relates to is closed. Data is also deleted upon deletion of the user account.

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, if applicable, 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

No third-party sub-processor is involved in delivering the Product.

International Transfers of Personal Data

The product can be configured to restrict the sending of certain data to Symantec, and customers may also use a firewall to block information from being sent to Symantec.

You are advised that, if necessary for service delivery or on customer instruction, Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, including potentially 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

Data stored on premise and that is not sent to Symantec's Global Intelligence Network (GIN) remains under the full control of the Customer.

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

Data stored on disk is encrypted. Data transferred to Symantec is encrypted in transit and subject to access control by dual factor authentication on the Symantec end.

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.
* For further information on the Personal Data processing involved in the use of other Symantec products referenced in this Notice, please refer to those products' Transparency Notices on the Symantec Privacy - GDPR Portal.