Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Security Analytics

This Privacy Transparency Notice describes how Security Analytics ("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

Security Analytics provides Customers with the ability to perform full packet capture with data enrichment for network security forensic investigation. The product has profiling capabilities for end user behavior, for the purpose of anomaly detection in the legitimate interest of network and information security.

Further information about the Product is available at:

https://www.symantec.com/products/network-forensics-security-analytics

2. Personal Data Collection And Processing

Sources of Data

Symantec may process four types of information from the Customer:

(1) High-level product usage information such as product features used, product version, and product performance provided in anonymized form via opt-out telemetry services.

(2) Signatures for previously-unknown malware along with a high-level score may be provided to the Symantec Global Intelligence Network via an opt-in telemetry service.

(3) Customer service reports may manually be submitted to Symantec Customer Support for diagnosing system failures. These reports contain system configuration information and system logs.

(4) Customer may submit captured packet data (PCAPs) to Symantec for diagnosing problems that cannot be reproduced by Symantec Customer Support or engineering. The content of these PCAPs is determined by the Customer, and may contain Personal Data.

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
Any Personal Data transmitted in an unencrypted network flow which the customer decides to route via the point of capture where the Product operates	Customer employees and contractors, any other individuals who interact in or with the customer's environment, or whose	Network security forensic investigations

	Personal Data is contained in captured network flows	

Personal Data Retention Schedule

The retention period for captured network traffic and generated metadata varies with the rate of network traffic ingestion. Captured network traffic and generated metadata are stored in fixed storage pools with a wrap-around technology whereby the oldest data is replaced with the newest data on a continual basis. 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

Data submitted to Symantec will be transferred or accessed (including for storage, backup and archiving) to the U.S.A. You are advised that Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, including potentially to external recipients, based on European Commission Decision C (2010)593 on Standard Contractual Clauses (processors), or of any alternate, legally permitted means.

4. Exercise Of Data Subject Rights

Customers may perform a reset to erase captured network traffic & generated metadata at any time. 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

It is Symantec's and all 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.