Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Security (SES)

This Privacy Transparency Notice describes how Symantec Endpoint Security ("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

The SES cloud portal introduces advanced visibility and controls to detect and remediate emerging threats in the customer's environment. The cloud portal also leverages Symantec Endpoint Protection*'s advanced machine learning capabilities to provide visibility into suspicious files and intensive policy-based control of anti-malware. Advanced machine learning does not require signatures to make sure that threats are stopped in your environment.

The following is a high-level summary of the features:

- Discover and block suspicious detections with the Intensive Protection policy
- Product configuration to optimize for low-bandwidth environments
- Integrated false management with central blacklist and whitelist
- Modern cloud portal for managing advanced features

With an intuitive cloud console, the product bulletproofs applications, or any software, such as productivity tools and browsers, offering auto-classification of risk levels of all endpoint applications whether or not they're in use, and application isolation to limit exploits.

Further information about the Product is available at:

https://www.symantec.com/products/endpoint-protection

2. Personal Data Collection And Processing

Sources of Data

SES collects the personal data in form of asset inventory, op-state and events from agents installed on Customer environment. Agents push this information directly or via hub installed on Customer site.

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 details (email, mobile number)	Customer end-users (typically employees and contractors)	User and device enrollment in the Product and registration in the customer account, generation of user certificates

		for secure network communications, installation and setup guidance, license administration, association of events to known users to reflect device health and risk status
Online identifiers (MAC address, unique device ID, device serial number, IMEI, username, password), device properties (OS version and model, installed applications, specific devices configurations)	Customer end-users (typically employees and contractors)	Device enrollment, active device inventory and management, detection of security events and cyber threats present on the networks to which enrolled devices connect
Network activity data, location and trackers (IP addresses, device identifiers, network identifiers and locales, host/usernames, browsing activity telemetry, session logs, traffic data, electronic communications data and metadata, cookies and similar)	Customer end-users (typically employees and contractors)	Detection and logging of, and protection against, phishing, scam, spam attempts and other security incidents; user notification of malicious networks and security events near the user's location

The Product does not need and is not meant to collect or process any Special Categories of Personal Data. In particular the Product is not directed to persons under 13, and we do not knowingly collect Personal Data from children under 13. If you become aware that a child under your care has provided us with Personal Data without your consent, please call customer support. We will take steps to remove the information and to terminate the child's account.

Personal Data Retention Schedule

Individual identifiers and contact details are retained for 30 days after the termination of the contractual relationship. Security event data is purged after 60 days. Online identifiers and trackers are deleted after contract termination. For the duration of the contractual relationship with the Customer, other Personal Data transmitted by the customer to Symantec is retained as described in the applicable product description / service terms. 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)	Individual identifiers, contact information, online identifiers and trackers	Services are deployed on AWS Infrastructure.	U.S.A. (East Coast)

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 your Product is configured to be provisioned to contain all Personal Data in the U.S.A. (East Coast). Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, including 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

Pursuant to the applicable Data Processing Addendum, and to the extent possible considering 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 is storing data in encrypted form with due access control in place. 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, considering 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.