Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Cloud Connect Defense

This Privacy Transparency Notice describes how Symantec Endpoint Cloud Connect Defense ("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 Endpoint Cloud Connect Defense is a multi-tenant cloud-based service. It protects endpoints from a variety of network threats, such as man-in-the-middle attacks, rogue wi-fi hotspots, low reputation wi-fi hotspots, content manipulation attacks, TLS/SSL traffic decryption and inspection, TLS/SSL traffic stripping, and active eavesdropping. The product also includes an app that is installed on endpoint devices.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

When devices are enrolled into the Product through the app, a record of the device is created with the associated device identifiers and the end-user who enrolled the device. As end-users connect their devices to various networks (e.g. wi-fi hotspots), active testing of each network is performed to determine whether network-based threats are present.

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
User identifiers (email addresses)	Customer's end-users (employees, contractors, other users of the Customer's devices)	Enrollment of devices in the Product and generation of user certificates for secure network communications
Device identifiers (IP address) and location data; identifiers of the networks to which enrolled devices connect	Customer's end-users (employees, contractors, other users of the Customer's devices)	Detection and recording of cyber threats present on the networks to which enrolled devices connect

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

Personal Data Retention Schedule

User specific data collected by the Product is removed when the device is un-enrolled. Moreover for the duration of the contractual relationship with the Customer, Personal Data is retained as described in the applicable product description. Accordingly, all device and user specific data is purged when the Customer terminates their service/account. After the expiry or termination of the contractual relationship, remaining Personal Data, if any, 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)	User, device, network identifiers, device location data	Device enrollment and network threat detection and recording	U.S.A.

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

The Customer can obtain the erasure of user specific data by un-enrolling the user's device from the Product. Additionally, except for data encoded in user certificates which are not editable in order to preserve certificate integrity and authentication security, user information can also be edited or removed by Symantec upon the Customer's request.

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

All communications from enrolled devices to the Symantec service are TLS encrypted (HTTPS). Authentication and authorization are provided using authentication tokens provisioned during

enrollment, then periodically refreshed. The Symantec service validates the device's token and scopes access based upon its authorization and control system. All data stored in AWS is encrypted at rest. The data and services are also protected via AWS Security Groups.

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.