

# Product Transparency Notice

For any queries, please contact [privacyteam@symantec.com](mailto:privacyteam@symantec.com)

## Symantec Endpoint Detection and Response (EDR) 4.0

This Privacy Transparency Notice describes how Symantec Endpoint Detection and Response 4.0 (commonly “Product”) collect and process 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 either version of the Product.

### 1. Product Description

Symantec EDR includes an on-premise appliance that monitors the activity of an entire organization, collecting forensics data and searching for suspicious activity. Symantec EDR also includes a cloud service. To improve their effectiveness, both the on-premise and the cloud option of the Product have the capability to continuously transmit the telemetry information they collect to Symantec over SSL, where the telemetry will be pulled down to hardened internal Symantec servers and used to support dashboards and queries requested by the Customer’s authorized personnel. The Customer however may freely choose to not use this functionality by disabling it.

Further information about the Product is available at:

<https://www.symantec.com/products/endpoint-detection-and-response>

### 2. Personal Data Collection And Processing

#### Sources of Data

The Product collects telemetry data related to endpoint device activity throughout the environment in which it is deployed by the Customer, including but not limited to accessing suspicious internet locations, running suspicious unverified applications, or executing trusted software in suspicious ways.

#### Respective Roles of Symantec and Customer

With respect to data collected, stored and processed within the Customer’s environment and not transmitted to Symantec, the Customer is the Controller.

With respect to Personal Data, if any, 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 (usernames), network activity data (log-ins, log-outs, internet browsing, suspicious network traffic)	Employees, contractors, other users of the Customer’s I.T. environment whose Personal Data may incidentally be contained in the telemetry collected by the Product.	Detect malicious activity threatening the security and privacy of the Customer’s organization and users

The Product does not need and is not meant to collect or process any Special Categories of Personal Data in the meaning of Article 9 of the European General Data Protection Regulation (GDPR).

#### Personal Data Retention Schedule

The data collected by the Product may be stored for up to 6 months. With respect to Personal Data, if any, transmitted from the Customer to Symantec for the purposes of the Product, for the duration of the contractual relationship with the Customer, the 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 may send Personal Data to internal recipients (affiliated Symantec entities) in the facilitation or provision of the Product. Symantec data centers supporting the Product are located in Germany and the United States.

#### Third-Party Sub-Processors

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

#### International Transfers of Personal Data

You are advised that as and if necessary, Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area 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

Telemetry data collected by the Product is viewable and searchable from the Product console. Access to this console is configured by 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

It is Symantec's and all of its affiliated entities' commitment 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.