

Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

End Point Detection and Response Cloud (EDRC)

This Privacy Transparency Notice describes how End Point Detection and Response Cloud (“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

End Point Detection and Response Cloud detects threats on individual endpoints by collecting and analyzing select customer-defined metadata.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

The personal data is collected by a dissolvable executable that is pushed to individual endpoints. That executable is pushed by an on-premises component that the customer installs inside their own network. The customer then decides the type of data to collect and when or how often to collect it.

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
Contact information (email address)	Customer employees and contractors	To enable login and password reset
Online identifiers and trackers (IP addresses and similar identifiers, cookies and other device trackers, product settings), network activity data (browsing activity, telemetry, session logs, traffic data) as configured by the customer	Customer’s employees, contractors, as well as other persons interacting electronically in or with the customer’s networks	To detect cybersecurity threats
Communications data (malicious contents conveyed through electronic)	Customer’s employees, contractors, as well as other persons interacting	To detect cybersecurity threats and to help respond to incidents

communications and web forms)	electronically in or with the customer’s networks	
-------------------------------	---	--

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

Personal Data Retention Schedule

Online identifiers and trackers and network activity data are retained for 30 days. Communications data is kept according to the data management and retention settings defined by the Customer.

For the duration of the contractual relationship with the Customer, other 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 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 (AWS)	Contact information, online identifiers and trackers, network activity data	Secure hosting	U.S.A. (future releases will include EU and/or UK-based hosting options)

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

Currently data will be transferred or accessed (including for storage, backup and archiving) in 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 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

Symantec EDRC can erase data upon Customer request, however records in logs are collected by the product programmatically/forensically and can therefore not be altered (amended or rectified) as that would compromise the integrity and reliability of the records.

Further, 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 EDRC takes measures for Information Security. All Personal Data is encrypted in transit and at rest. Controls such as access control and least privilege are implemented to protect personal data. 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.