

Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Integrated Cyber Defense Manager (ICDm)

This Privacy Transparency Notice describes how Symantec Integrated Cyber Defense Manager (“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 Integrated Cyber Defense Manager (ICDm) is a unified cloud console that provides complete threat visibility across the Customer’s endpoints and leverages multiple technologies to manage the security posture of the Customer’s organization. It allows managing various Symantec products for which the Customer has a license. The products currently available in ICDm include Symantec Endpoint Security*, Symantec Endpoint Cloud Connect Defense*, Symantec Endpoint Application Isolation*, Symantec Endpoint Application Control*, as well as Symantec Data Loss Prevention Cloud*, Symantec Endpoint Detection Response (Cloud)* and Symantec Endpoint Security Complete*.

ICDm also enables security orchestration and automation leveraging the Flowable workflow tool. Flowable provides a core set of open source business process engines that are compact and highly efficient. They provide a workflow and Business Process Management (BPM) platform for developers, system admins and business users, including a Business Process Model and Notation (BPMN) process engine, accompanying Decision Model and Notation (DMN) decision tables and Case Management Model and Notation (CMMN) engines.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

The Product only collects Personal Data fed into it by the Customer and by Customer-assigned end-users, including through the use of other Symantec products available in ICDm, as described earlier. For further information on the Personal Data collected by such other products, please refer to their respective Transparency Notices on the [Symantec Privacy - GDPR Portal](#).

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), contact information (email addresses), online identifiers	Customer admins and end-users	Licensing, provisioning and user management;

(usernames), credentials (passwords)		Access to, configuration and use of the service; Login and synchronization; Communication of Customer-generated reports to Customer-selected recipients; Tracking of product usage
Network and device identifiers (device IDs, IP addresses and MAC addresses) and device geolocation data; any user-identifying data (e.g. user ID) incidentally contained in directory names associated with application and file information	Enrolled users of the Customer	Device enrollment, asset inventory and duplication prevention; Customer-initiated network discovery; Policy definition and rule-setting; Asset and event logging and reporting

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

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. Any Personal Data fed by the Customer (i.e. by the Customer’s admins and end-users) into a workflow will be purged upon successful completion of that workflow.

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

If and as necessary, 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 (cloud deployment only) are:

Sub-Processor	Personal Data	Purpose of processing	Locations
Amazon Web Services (AWS)	All of the above	Hosting on third party 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 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 as the Controller has the ability to input, amend or remove the Personal Data it feeds into the Product.

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

Personal Data processed by Symantec on behalf of the Customer for the purposes of the Product is encrypted both at rest and in transit.

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.

* For further information on the Personal Data processing involved in the use of other Symantec Products or Services referenced in this Notice, please refer to those Products' or Services' Transparency Notices on the [Symantec Privacy - GDPR Portal](#).