Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Advanced Threat Protection Endpoint (Hosted Service)

This Privacy Transparency Notice describes how Advanced Threat Protection Endpoint (ATP Endpoint) ("Hosted Service") 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 Hosted Service.

1. Product Description

Advanced Threat Protection Endpoint provides full endpoint visibility and real-time queries via continuous recording of system activity on the endpoints. The Hosted Service leverages the integrated Endpoint Detection and Response capabilities in Symantec Endpoint Protection (SEP)*. It gives customers the tools to expose, contain and resolve breaches resulting from advanced attacks. The Customer can access the Hosted Service through a self-service online portal. The Customer may configure and manage the Hosted Service, access reports, and view data and statistics, through the portal.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

The Hosted Service collects system activity data from the Symantec Endpoint Protection (SEP)* product deployed on endpoints in the Customer's environment. Some of this information can be correlated to individuals by the use of IP address, and occasionally company usernames. This information may also be correlated with web browsing activity and with applications downloaded and run.

Optionally the Customer can opt for the Hosted Service to submit telemetry data to Symantec for the purpose of improving the detection of, and protection against cybersecurity threats. Such telemetry data is anonymous and does not contain Personal Data such as usernames, IP addresses, emails, machine identifiers or any data that is relatable or attributable to an individual.

Respective Roles of Symantec and Customer

With respect to Personal Data transmitted from the Customer to Symantec for the purposes of the hosted Service, 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 (usernames), credentials (passwords) and contact	Customer employees and contractors	Identification and authentication of users, access to the service portal

information (e.g. email addresses)		
Event and incident data, i.e. network activity data (browsing activity, session logs, traffic data and related telemetry), application data about executables downloaded and launched on monitored equipment, other data submitted by the Customer	Customer employees and contractors, other individuals interacting in or with the monitored endpoint devices	Detection of and protection against cybersecurity threats, implementation of Customer-defined computer use policy (or equivalent)

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

Personal Data Retention Schedule

Customer data in the Hosted Service undergoes a full back-up on a daily basis. Two generations of those back-ups are kept. Event and incident data are managed automatically and purged automatically whenever storage space is required.

3. Disclosure and International Transfer of Personal Data

Third-Party Sub-Processors

The third-party sub-processors involved in delivering the Hosted Service are:

Sub-Processor	Personal Data	Purpose of processing	Locations
Amazon Web Services	Individual identifiers, credentials, contact information, event and incident data, any other data submitted by the Customer	Cloud hosting	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

Customers can freely create, edit and manage users through the service portal, and have full access to the event and incident data stored by the Hosted Service.

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

The Hosted Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Hosted Service is regularly monitored for service level compliance and adjustments are made as needed. Reporting for the Hosted Service is available through the Portal. Reporting may include activity logs and/or statistics. The Customer may choose to generate reports through the service portal, which can be configured to be sent by email on a scheduled basis, or downloaded from the portal.

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 Hosted Service. 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.