Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Protection Engine 8.0 for Cloud Services & Network Attached Storage - With Cloud Console (SPE 8.0)

This Privacy Transparency Notice describes how Symantec Protection Engine 8.0 for Cloud Services & Network Attached Storage - With Cloud Console ("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 Protection Engine (SPE) is an application that allows customers to incorporate malware and threat detection technologies into almost any application on Windows & Linux. SPE typically helps various applications or file storages in scanning the data at rest as well as on wire. SPE is available to customers in two separate SKUs viz. Symantec™ Protection Engine for Cloud Services (SPE for CS) and Symantec Protection Engine for Network Attached Storage (SPE for NAS).

SPE for CS enables customers to secure their applications/data exposed to the web. It also enables them to integrate its malware scanning capability in any application that supports scanning of files over ICAP protocol. SPE for NAS allows customers to protect data saved, getting stored in & retrieved from NAS storages of various brands. The newest version of SPE can be used in either standalone mode (just like its earlier SPE* versions 7.9 and below) or in Centralized Management mode (introduced in 8.0).

With Centralized Management mode, it will be possible for the customer to manage the SPE instance along with other SPE instances in their enterprise network from a single Cloud based console. Symantec's cloud console is an internet facing online portal available globally. Customers will have to onboard (signup to) the console & sign into it. Then, they will have to configure the SPE instances in Centralized Management mode, enroll them in the console & start using the management facilities provided by the console. Customer information is gathered at the time when customer onboards or signs up on the Cloud Console. Also, the enrolled SPE instances send events of malware detection & remediation actions to Cloud Console so that they can be viewed by the customer from a single place/page.

SPE shares the cloud console with other Symantec applications like Cloud Workload Protection* & Cloud Workload Protection for Storage*. For Live Update, Protection Engine uses Live Update Administrator* if configured by the customer.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

SPE collects information such as email metadata (id, domain, subject, etc.) to filter emails according to the policy configured by the customer. This information is stored in SPE local logs which reside on the machine on which SPE is deployed and hosted. This hosting machine always remains in the customer's enterprise network and the information is not transferred to

Symantec's backend systems in the cloud, so the customer keeps complete control over this information.

For using Centralized Management features, when customers onboard on Symantec's Common Cloud console, they need to provide a minimal amount of personal details in the onboarding page (first name, last name, email ID), which will be processed by Symantec I.T. to complete the onboarding of the customer. Other details required for onboarding like the customer's company name, address and phone numbers are collected from Symantec's customer database based on the License Key sent to the cloud from the OnPrem SPE setup. SPE also collects non-personal install time and runtime telemetry data of the deployed product and transmits it to the Symantec Telemetry Server.

SPE internally integrates various security/anti-malware technologies from Symantec Security Technology and Response (STAR)*. Details about files scanned are collected by STAR components and submitted to Symantec backend systems for the purpose of improving malware detection. If configured, Symantec's Central Quarantine Server* helps SPE to maintain quarantined malware files at a central location.

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 (name) and contact information (email address)	Customer employees and contractors	Customer onboarding and user enrolment. The console accepts name of the user and email address (optional) while creating the user in the management console. SPE's Java applet based Management Console supports multiple users to manage it. Enrolled email-id is used to notify events.
Electronic communication data (email metadata)	Customer employees and contractors, other entities interacting with the customer	Configuration and enforcement of the customer's email filtering policy
Online identifiers (IP addresses, Service Set Identifiers)	Customer employees and contractors, clients and suppliers, other entities interacting with the customer	Discovery and protection of the customer environment. NAS Filer IP, NAS Filer Client IP and Client Application IP are used in event notifications. For NAS (NetApp), SSID of the user who accessed files is logged in local SPE logs.

		For NAS (NetApp used by Customer in Cluster mode), VServer IP is logged in local SPE logs.

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

Personal Data Retention Schedule

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

Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and external recipients (third party sub-processors) as necessary for 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)	Individual and online identifiers, contact information	The services are deployed on AWS infrastructure. Note: In their account, customers can configure Cloud Workload Protection to send event data to Amazon CloudWatch.	U.S.A., EU (Frankfurt)

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

Customer can request to amend/rectify or delete the data collected by Cloud Workload Protection for the purposes of Symantec Protection Engine.

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

SPE Log files are protected based on filesystem ACL and logs are retained for 365 day (configurable). All temporary data is cleaned before the process is stopped. All SPE log files are collected and maintained on the system on which SPE is installed. These systems are running in the customer's enterprise network. Data such as log files are not sent back to any of Symantec's backend services without intervention of the customer. Therefore the customer has complete ownership and control over these log files and can destroy them or clean them up discretionarily. All data transfers happen on a secure https/SSL channel. All data stored in a secured data store. Only Symantec authorized personnel have access to the secure data store, where customers' sensitive data is stored in encrypted form.

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 referenced in this Notice, please refer to those products' Transparency Notices on the Symantec Privacy - GDPR Portal.