Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Cloud Workload Assurance

This Privacy Transparency Notice describes how Symantec Cloud Workload Assurance ("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 Cloud Workload Assurance (CWA) provides a single dashboard to pro-actively manage cloud security risk by minimizing attack surface and improving the overall security posture of your cloud infrastructure. Cloud security brings in a unique set of security concerns because of the service models and deployment models that can be adopted. This makes it necessary to follow security configuration best practices specific to the cloud environment. To counter the vulnerability threats surfacing on a continuous basis, assessment of security compliance must be an ongoing activity. CWA is an automated compliance tool that helps you secure your cloud infrastructure and achieve these business objectives. CWA is part of Symantec's Cloud Workload Protection* suite (CWP).

Further information about the Product is available at:

https://support.symantec.com/en_US/product.cloud-workload-protection.html

2. Personal Data Collection And Processing

Sources of Data

CWA collects customer email ID during product enrollment from common cloud. This is used to login to the CWA web portal hosted on Amazon Web Services (AWS). Once logged in to the portal, the customer can configure what AWS account to scan. As a part of configuration, the customer needs to create role with required privileges in the 'customer AWS' account, and give permissions to the 'Symantec AWS' account to access the 'customer AWS' account through ExternalRole.

CWA product collects a range of AWS resources, which currently include: Virtual Private Cloud ('VPC'), security group, cloud watch, Identity & Access Management ('IAM': password policy, IAM users, cloud trail), Amazon Resource Name ('ARN': resource region and other properties).

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, email ID)	Customer employees and contractors	Identification of registered users
Contact information (address, phone)	Customer employees and contractors	Customer communications

Online identifiers and trackers (usernames, device IDs and similar unique identifiers, service settings and preferences)	Customer employees and contractors	Discovery of the customer's AWS resources and security assessment of the customer's environment

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 identifiers, contact information, Online identifiers and trackers	IaaS 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 as necessary for service delivery, 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

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

All data transfers happen on secure https/SSL channel. All data is held in secured data store. Only Symantec authorized personnel have access to the secure data store. Customer 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.