

# Product Transparency Notice

For any queries, please contact [privacyteam@symantec.com](mailto:privacyteam@symantec.com)

## Symantec Cloud Workload Protection (CWP)

This Privacy Transparency Notice describes how Symantec Cloud Workload Protection (“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 Protection automates security for public and hybrid cloud workloads, enabling business agility and DevSecOps workflows for enterprises. CWP integrates natively with AWS to provide elastic, scalable workload security and has achieved Security Competency. It discovers and maps the blind spots in public cloud deployments. The single cloud-based console protects workloads across public clouds, private clouds, and physical on-premises data centers. CWP provides the industry's first cloud-native real-time anti-malware scanning to help keep compute instances free of threats using the latest Symantec Endpoint Protection\* (SEP 14) anti-malware technologies.

Further information about the Product is available at:

<https://www.symantec.com/products/cloud-workload-protection>

### 2. Personal Data Collection And Processing

#### Sources of Data

Data is collected at the time of product enrolment from common cloud or AWS marketplace. After completion of the cloud platform configuration is done, it pulls cloud platform details from the cloud platform. CWP Agent also collects information from instance and storage scanner.

#### 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 and company identifiers (names) and contact information (email, phone, address)	Customer employees, contractors, clients, suppliers	To identify users registered with product services
Online identifiers and trackers (IP addresses, host/user names, device IDs, cookies)	Customer employees, contractors, clients, suppliers	To discover and protect the customer environment
Network activity data (browsing, session logs, telemetry, traffic data)	Customer employees, contractors, clients, suppliers	To protect the customer environment and alert to security events

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

**Personal Data Retention Schedule**

Personal Data collected for identifying registered users is erased 30 days after subscription expiry or cancellation. Events data is erased after 90 days. 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), 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
AWS	Individual identifiers, contact information, online identifiers and trackers	Services are deployed on AWS Infrastructure. CWP can be configured to export the events to AWS CloudWatch in customer account.	U.S.A.
Azure	Online identifiers and trackers	Ease of agent deployment via Azure VM extension	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, 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**

Customer can request to amend/rectify or delete the data collected by CWP. 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 authorized personnel have exclusive access to the secure data store. All the data is transferred on secure https/SSL channel and stored in secured data store. Customer sensitive data is stored in encrypted form. 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.

\* 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](#).