Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Data Center Security (DCS)

This Privacy Transparency Notice describes how Data Center Security ("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 involved in using the Product.

1. Product Description

Symantec's Data Center Security monitors and protects critical servers and systems for security violations and anomalies that could leads to a compromised state of the system.

Further information about the Product is available at:

https://www.symantec.com/products/data-center-security

2. Personal Data Collection And Processing

Sources of Data

Data is collected based on policy applied to each protected system. Data Center Security agent is deployed to each system and it monitors security violations and anomalies and reports back to a server installed on premise in Customer environment.

Respective Roles of Symantec and Customer

With respect to Personal Data collected by the Product during its use, the Customer is the Controller. The use of the Product does not involve Symantec as a Data Processor.

With respect to any Personal Data transmitted from the customer to Symantec for the purposes related to the Product (e.g. support), the Customer is the controller, and your Symantec contracting entity as specified in your applicable Agreement ("Symantec") acts as a processor. For such cases 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
File and Registry access by users via active processes (filename, user ID, action performed, process used)	Customer employees and contractors	To determine possible security access violations and allow/deny access according to security policy
User and Group Activities (new user/group creation, changes to user/group, login success and failure events)	Customer employees and contractors	To determine possible security access violation
Contact information (email address)	Customer employees and contractors	To send security alerts
Network Connections (local IP address/port, remote IP address/port, user/process associated to the connection)	Customer employees and contractors	To determine possible security access violations and allow/deny access according to security policy

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

Personal Data Retention Schedule

Security Data collected which may contain Personal Data for determining possible security intrusion on system could be retained for 7 - 550 days adjustable by customer and erased afterwards.

As regards any Personal Data the customer may choose to transmit Symantec, for the duration of the contractual relationship with the Customer, Personal Data is retained as described in the applicable product description / service terms. 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 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

During its normal operation, the Product does not transmit data to Symantec. As regards any Personal Data the customer may choose to transmit Symantec, Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and, if applicable, external recipients (third party sub-processors). The list of Symantec affiliated entities and their geographical locations are available on the Symantec Privacy - GDPR Portal.

Third-Party Sub-Processors

No third-party sub-processor is involved in delivering the Product.

International Transfers of Personal Data

During its normal operation, the Product does not transmit data to Symantec. As regards any Personal Data the customer may choose to transmit Symantec, you are advised that Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, potentially 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

Data collected by Data Center Security is stored in MSSQL database owned, configured and managed by the customer. It is located on premise of the customer and the customer has full authority and ability to modify the data collected by Data Center Security product.

5. Information Security

Technical and Organizational Measures

Data collected by Data Center Security is stored on Customer's system on premise. Symantec has no access to it. As regards product design, and as regards any Personal Data the customer may choose to transmit Symantec, 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.

Document Version 1.2
Date of issue: May 12, 2018