Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

SSL Visibility Appliance (SSLV)

This Privacy Transparency Notice describes how SSL Visibility Appliance (SSLV) ("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

SSLV is an appliance based transparent proxy for SSL network communications. SSLV acts as a policy control point enabling explicit control over what SSL traffic is and is not allowed across the network, and enables other security appliances to see decrypted data from selected encrypted traffic crossing the network. It does this using well known mechanisms to decrypt encrypted traffic. The purpose of SSLV is to allow the customer to control the encrypted traffic within their network and where appropriate to make the decrypted content of encrypted traffic visible to security tools within the customer's network.

Further information about the Product is available at:

https://www.symantec.com/products/ssl-visibility-appliance

2. Personal Data Collection And Processing

Sources of Data

No data is collected or stored for network traffic inspected by the appliance under normal operation. Management interface access by operators is logged and operators can invoke troubleshooting mechanisms that may capture decrypted user data. Managers log onto the management interface and logon information is captured. Troubleshooting tools allow capturing of PCAP files that may contain decrypted traffic for traffic passing through the appliance.

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.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Contact information (email)	Customer employees and contractors	Notification of system alerts
Online identifiers and trackers, network activity data (management interface audit logs, session activity logs), and related communications data	Customer employees and contractors, other individuals interacting in or with the customer's environment	Servicing and troubleshooting purposes
Any Personal Data in traffic which the customer decides to route via to the appliance	Customer employees and contractors, any other individuals who interact in or with the customer's	Packet Captures (PCAPs) for the management or data interfaces

	environment, or whose Personal Data is contained in traffic routed to the appliance	

Personal Data Retention Schedule

The creation of a PCAPs is initiated by the user via the Web User Interface of the product. The PCAP is stored on an encrypted portion of the SSLV SSD. Transmission of the PCAP is fully optional by the customer. If provided by the customer, corresponding SSLV Case Evidence (PCAPs), are uploaded or transferred to Symantec's Managed File Transfer (MFT) servers.

As the Controller, the customer is solely responsible for defining and implementing the retention policies and periods applicable to Personal Data collected through the use of the Product and held in the customer's environment.

Regarding data transmitted to Symantec, 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

If the customer chooses to provide PCAP files, the data is stored on Symantec's Managed File Transfer (MFT) secure storage tool in the U.S.A. The data is used by Symantec Customer Support located in either the U.S.A., Canada, or the Asia-Pacific region, to troubleshoot issues upon customer request. In some cases, Customer Support may share the data with Product Engineering located in the USA for help with troubleshooting.

Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and, if applicable, 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

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

International Transfers of Personal Data

Data will be transferred or accessed (including for storage, backup and archiving) to USA. 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

For SSL session logs, the customer can control which, or whether any sessions are logged, and selected portions can be exported. PCAP files can be exported and modified by the customer in third-party tools. The customer can also request that Symantec Customer Support delete their case evidence.

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

Symantec processes and procedures prohibit personnel from making any copy of any customer data stored on hardware products. The storage devices are wiped during the installation of the SSLV software. No personal data is made available to anyone servicing or repairing hardware devices. Faulty products deemed unrepairable will be mechanically destroyed and scrapped.

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.