Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Proxy Secure Gateway (ProxySG - ASG)

This Privacy Transparency Notice describes how Proxy Secure Gateway ("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

The primary purpose for the Proxy Secure Gateway is to enable the end customer to control access to the internet and provide security for that access through a variety of methods including information from Symantec's Global Intelligence Network service as well as information and analysis from external Internet Content Adaptation Protocol based services such as Content Analysis and Data Loss Prevention.

Further information about the Product is available at:

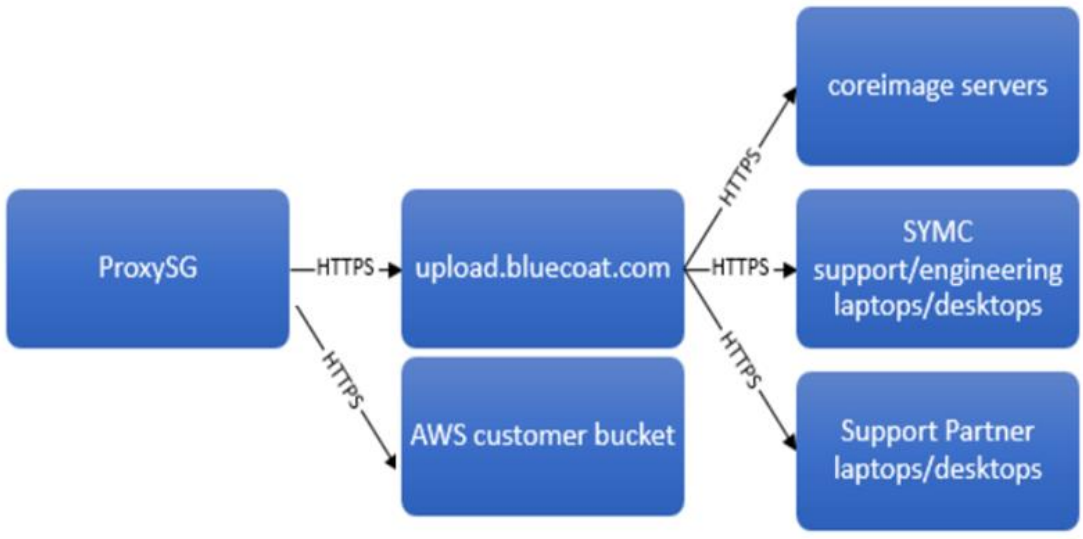
https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg

2. Personal Data Collection And Processing

Sources of Data

The product's purpose is not to collect or process Personal Data. The product does collect diagnostic data to facilitate debugging. No Customer Personal Data is sent back to Symantec and the product does not send any other Personal Data automatically.

Customers can choose to send to Symantec diagnostic data such as core dumps, system information, access logs, troubleshooting logs (ASG only) and event logs. hat may contain Personal Data and has been collected by the product. This is done as part of a support investigation. The following diagram illustrates diagnostic data collection and distribution within Symantec.



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 normally involve Symantec as a Data Processor.

However for any Personal Data transmitted by the Customer to Symantec for the purposes of support investigation, 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, contact information, location data, online identifiers, network activity data and communication data	Customer employees, contractors and clients	Access logging, diagnostics, debugging and resolution for Customer issues with the product

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

Personal Data Retention Schedule

Access log data remains in the Secure Gateway until it is either uploaded or overwritten by new entries. The diagnostic data is retained only until the maximum number of that data type is uploaded.

Customer Information data is retained until the account is deleted. Individual identifiers on upload.bluecoat.com are retained for up to 2 years or when the associated support case has been closed for 2 months. The core servers retain the data if space permits or until the associated Engineering bug has been closed for a year. Data downloaded onto individual's devices remains until manually deleted.

The customer can choose to continuously upload the access log data from the Secure Gateway or to upload it once a certain size is hit. Once uploaded the data is deleted from the product. If the customer does not upload the access log they can specify to overwrite old entries with new ones or stop logging when the log is full. Other diagnostic info (cores, snapshots) etc. will eventually overwrite themselves as there are limited slots/number of each type of which the Secure Gateway maintains a list. Some items such as the core files can be explicitly deleted by the Customer.

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

Symantec involves no third-party sub-processor in delivering the Product to the Customer.

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

Customers will not be able to access, rectify or erase the personal data uploaded by the product for diagnostic purposes. The data is stored and processed on devices that customers cannot access directly. Customers can contact Symantec and ask that their data be updated or deleted.

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

Upload.bluecoat.com access is restricted to those employees and partners that require access to perform diagnostic of Customer issues. The data is not encrypted itself. It is secured in transit and is transferred using HTTPS.

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.