FORCEPOINT
POWERED BY Raytheon

Forcepoint Email Security Hybrid Management of Personal Data

Forcepoint Email Security Hybrid – Management of Personal Data

CONTENTS

Disclaimer

This document contains information regarding Forcepoint products and/or services. The information is Forcepoint's property. While every effort was made to ensure the content is up-to-date and accurate, the information is provided AS IS, without any representation or warranty, express or implied, and is subject to change without notice. Any references to future releases or functionality are forecasts and not intended to be commitments. Forcepoint assumes no liability for the use of this information.

General

Document Purpose

This document is designed to answer the question: “What personal data is stored in the cloud infrastructure when using Forcepoint Email Security Hybrid (formerly TRITON AP-EMAIL Hybrid)?” It is primarily intended for those involved in the procurement and privacy assessment of the Forcepoint Email Security Hybrid product.

Note: For Forcepoint Email Security Cloud deployments (formerly TRITON AP-EMAIL Cloud), please see separate product-specific documentation.

Forcepoint Cloud Trust Program

This document forms part of the wider Forcepoint Cloud Trust Program. Details available at https://www.forcepoint.com/forcepoint-cloud-compliance

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was adopted on April 27, 2016 and came into effect on May 25, 2018. GDPR, which replaced the Data Protection Directive 95/46/EC, is a significant source for the privacy principles that guide Forcepoint’s privacy policies and processes, both internally and externally. Full details of the GDPR can be found in various sources, including https://ec.europa.eu/info/law/law-topic/data-protection/reform_en

The operation of the Forcepoint Email Security Hybrid service is designed to comply with GDPR principles. Consistent with GDPR’s principles, Forcepoint’s customers and partners are the data controllers and Forcepoint is the data processor with respect to customer and partner data transferred to/from or stored in Forcepoint Email Security Hybrid’s infrastructure. As a data processor, Forcepoint uses industry-standard techniques consistent with identified risks to secure data held within its cloud infrastructure. Further, Forcepoint works collaboratively with its customers as necessary to meet GDPR requirements.

Personal Data

This document adheres to the definition of personal data as defined in article 4.1 of the General Data Protection Regulation, which defines 'personal data’ as any information relating to an identified or identifiable natural person (‘Data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Safeguarding Personal Data

Forcepoint uses industry-standard techniques to encrypt data held within our cloud infrastructure that has been identified as high risk, including personal data. This approach to data security ensures that the high-risk data is unintelligible to any person who is not authorised to access it. In addition, information in transit, whether across the Forcepoint network or public networks, is always encrypted using industry-standard techniques.

Identity & Policy

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
Policy	Security/acceptable use policy is defined by the customer administrator using the on-premise Security Manager. See Table 1: Email Policy Personal Data Attributes for further details.	To allow customer administrator defined security policy and acceptable use policy to be tailored to specific geographies, groups and/or individuals.	Policy definition data is defined in the on-premise Security Manager, it is then synchronised to and stored in the cloud data centers as configured by the customer.	During subscription term: - Policy data is retained until the next policy version is synchronized at which point it is updated and replaced by the new policy version. After subscription term: - Policy data is permanently deleted from the cloud infrastructure 6 months after the subscription has terminated.
Directory Data (Directory Sync)	Directory information is synchronized from the on-premise directory synchronization client to the cloud data centers. See Table 2: Directory Synchonization Personal Data Attributes for further details.	To allow end users to authenticate to the service and for the service to apply the correct security policy,	Directory data is replicated to, and stored in, the cloud data centers as configured by the customer on a schedule defined by the customer.	During subscription term: - Directory data is refreshed and replaced according to the directory synchronization schedule set by the customer administrator on the Directory Synchronization Client. After subscription term: - Directory data is permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.

Activity Logging

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
User Activity Logs (Download sync data)	User activity logs are created by the cloud infrastructure from the processing of inbound emails before they are routed to the customer on-premise system. The logs contain information related to emails processed including details of the sender, recipient, the subject and sending IP. See Table 3: User Activity Log Download (sync) Personal Data Attributes.	To provide granularity in the reporting system. To provide details of each email transaction, to allow customers to process the emails being received by their users.	User activity log data is first created in the cloud data centers to which the customer connects according to their MX record. The customer then copies the logs to their on-premise system using the log sync service on a schedule of their choosing, but within 14 days of the log creation date.	During subscription term: - User activity log files are retained in the cloud Infrastructure for 14 days, they are then removed permanently. After subscription term: - User activity log files are removed permanently from the cloud infrastructure 14 days after the subscription term has terminated.

Appendix **A**

TERMINOLOGY

Term	Explanation
Cloud data centers	Forcepoint's co-located, ISO27001 Certified, Tier 4 data centers.
Cloud infrastructure	Components and services within cloud data centers.
On-premise Security Manager	Forcepoint Security Manager, the management console for Forcepoint Email Security located on customer premises.

Table 1: Email Policy Personal Data Attributes

The following personal data can be found in a policy, subject to configuration.

Attribute	Requirement
Postmaster email address	Mandatory

Table 2: Directory Synchronization Personal Data Attributes

The following information can be synchronised from a customer's Active Directory.

Attributes	Requirement
CN (Common Name)	Mandatory
GUID	Mandatory
Email Address	Mandatory
NTML Identity	Optional
MailAlias(es)	Optional
Group Membership	Optional

Table 3: User Activity Log Download (sync) Personal Data Attributes

User Activity log data downloaded from the cloud infrastructure to the customer's Email Security on-premise system may contain the following personal data.

Attribute
Envelope Sender
Recipient Address
Subject
Sender IP (Log)