FORCEPOINT
POWERED BY Raytheon

Forcepoint Email Security Cloud Management of Personal Data

Forcepoint Email Security Cloud – Management of Personal Data

CONTENTS

Disclaimer 2
General 3
- Document Purpose 3
- Forcepoint Cloud Trust Program 3
- General Data Protection Regulation (GDPR) 3
- Personal Data 3
- Safeguarding Personal Data 3

Identity & Policy 4
- Cloud Portal Contacts 4
- Directory Data 4
- Policy 4

Activity Logging 5
- Email Activity Logs (REPORT CENTER) 5
- Email Activity Logs (LEGACY EMAIL REPORTS) 5
- SIEM Integration 5
- Cloud Portal Audit Trail 6
- Quarantined Email (including Personal Email Subscriptions) 6
- Attachment Parking 6
- Keep a Copy 6
- Standard Encryption 7

Add-on Modules 8
- Advanced Malware Detection 8
- Image Analysis Module 8
- Email Encryption Module 8

Appendix A 9
- Table 1: Cloud Portal Contacts Personal Data Attributes 9
- Table 2: Directory Synchronization Data Personal Data Attributes 9
- Table 3: Email Policy Personal Data Attributes 9
- Table 4: Report Center Personal Data Attributes 10
- Table 5: Legacy Reporting Personal Data Attributes 10
- Table 6: Audit Trail Personal Data Attributes 11
- Table 7: Quarantine Items Personal Data Attributes 11

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 Cloud (formerly TRITON AP-EMAIL Cloud)?” It is primarily intended for those involved in the procurement and privacy assessment of the Forcepoint Email Security Cloud product.

Note: For Forcepoint Email Security Hybrid deployments (formerly TRITON AP-EMAIL Hybrid Module), 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 Cloud 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 Cloud’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 authorized 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
Cloud Portal Contacts	Cloud portal contacts are created by the customer administrator. An initial contact is created as part of service provisioning, thereafter the customer is free to create and manage new contacts as required. See Table 1: Cloud Portal Contacts Personal Data Attributes for details.	For the purpose of providing and controlling customer administrative access to the service via the cloud portal.	Contact definitions are created in the cloud portal, stored centrally and synchronized with three other cloud data centers for redundancy.	During subscription term: - Contact definitions are held for the duration of the service subscription unless deleted by the customer administrator. After subscription term: - Contact definitions are permanently deleted from the Forcepoint cloud infrastructure 6 months after the subscription has terminated.
Directory Data *(Directory Sync)*	Directory information, when provided, is synchronized from the on-premise Directory Synchronization Client to the cloud data centers. See Table 2: Directory Synchronization Data Personal Data Attributes for 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 all cloud data centers as configured by the customer.	During subscription term: - Directory synchronization data is refreshed and replaced according to the directory synchronisation schedule set by the customer administrator via the Directory Synchronization Client. After subscription term: - Directory synchronization data is removed permanently from the cloud infrastructure 6 months after the subscription has terminated.
Policy	A policy can cover a number of items including service connection information / notification page definitions / security configuration / content filter and encryption. Policy information can also include block and allow lists for both individual users and groups. Customer entered Content Control classifiers could potentially contain personal data. See Table 3: Email Policy Personal Data Attributes for further details.	To allow security policies and acceptable use policies defined by customer administrators to be tailored to specific geographies, groups and/or individuals.	Policy definition data is created in the cloud portal, stored centrally and then synchronized with all of 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.

Activity Logging

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
Email Activity Logs (REPORT CENTER)	Email activity logs viewed in REPORT CENTER are created by the cloud infrastructure from the processing of inbound and outbound emails. The logs contain details about all emails processed including details of the sender, recipient, the subject and sending IP. See Table 4: Report Center Personal Data Attributes for further details	To provide granularity in the reporting system. To provide details of each email transaction, to allow customers to understand the emails being sent, and being sent to, their users.	Email activity log data for REPORT CENTER is first created in the cloud data center that the customer MX record connects to. It is then fed back to the customer selected cloud data center for storage and ultimately extraction by the customer. At the time of service set-up, customers can define the two geographic locations in which email activity log data is stored.	During subscription term: - As standard email activity logs older than 90 days are permanently deleted. - At subscriber's option, email activity logs may be retained in the cloud infrastructure for longer than the standard 90 day period if customer purchases any extended reporting options. After subscription term: - User activity log records are permanently deleted from the cloud infrastructure 90 days after the subscription has terminated or 6 months after the subscription has terminated if extended reporting options have been purchased.
Email Activity Logs (LEGACY EMAIL REPORTS)	Email activity logs viewed in the LEGACY EMAIL REPORTS menu are created by the cloud Infrastructure from the processing of inbound and outbound emails. The logs contain details about all emails processed including details of the sender, recipient and subject. See Table 5: Legacy Reporting Personal Data attributes	To provide granularity in the reporting system. To provide details of each email transaction, to allow customers to understand the emails being sent, and being sent to, their users.	Email activity log data for LEGACY EMAIL REPORTS is first created in the cloud data center that the customer MX record connects to. Email activity log data is retained in this cloud data center for subsequent access by the customer. Email activity log data accessed through LEGACY EMAIL REPORTS can be detailed or summary.	During subscription term: - User email activity log data accessed through LEGACY EMAIL REPORTS are retained in the cloud Infrastructure for a rolling 30 day period in the case of detailed logs, after which they are removed permanently. Summarized logs contain minimal personal data are retained for a longer period (up to two years), after which they are removed permanently. After subscription term: - User activity log records are removed permanently from the cloud infrastructure 30 days after the subscription has terminated.
SIEM Integration *(beta only)*	SIEM integration, when enabled by customer administrator can be used to create a feed of filtered reporting data pulled from the user activity logs.	Optionally used by the customer administrator to transfer user activity logs to customer's Security Information and Event Management (SIEM) systems.	SIEM integration records are extracted according to policy and filters created by the customer administrator for selected, or all, security policies. SIEM integration log data files exist transiently in the cloud data centers selected by the customer administrator for the account at service set-up. The customer pulls copies of the SIEM integration log data files to their premises using a software agent on a schedule of their choosing, but within 14 days of the log creation date.	During subscription term: - New SIEM log file entries are retained in the cloud web infrastructure for a rolling 14 day period before being automatically purged, whereupon they are removed permanently. After subscription term: - SIEM logs are removed permanently from the cloud web infrastructure 14 days after the subscription has terminated.

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
Cloud Portal Audit Trail	The cloud portal configuration audit trail records the administrative users (Contacts) that made changes to the cloud portal configuration, and details of those changes. See Table 6: Audit Trail Personal Data Attributes.	To provide traceability of cloud portal administrator activity.	Cloud portal audit trail records are stored in multiple cloud data centers selected by the customer administrator upon service set up. Personal data is not directly stored in the audit trail, instead links are provided to the cloud portal contact records (see above).	During subscription term: - As standard portal audit trail data older than 90 days are permanently deleted. - At subscriber's option, portal audit trail data may be retained in the cloud infrastructure for longer than the standard 90 day period if customer purchases any extended reporting options. After subscription term: - Portal audit trail data records are permanently deleted from the cloud infrastructure 90 days after the subscription has terminated or 6 months after the subscription has terminated if extended reporting options have been purchased.
Quarantined Email (including Personal Email Subscriptions)	Emails that are configured by policy to be quarantined either for review by an administrator (Quarantined Email) or a user (Personal Email Subscriptions) are retained in the Cloud Infrastructure until either released OR they age out and are deleted after 30 days. The whole email is retained in quarantine to allow the user the decision whether to release or not. See Table 7: Quarantine Items Personal Data Attributes below for details.	To provide administrator or the user with the flexibility of blocking perceived to be suspicious email from delivering to mailboxes.	Quarantined emails are identified in the cloud data center that the customer MX record connects to. They are retained in this cloud data center for review and release by the customer.	During subscription term: - Quarantined messages are retained in the cloud infrastructure for a maximum period of 30 days unless they are released earlier after which they are removed permanently. After subscription term: - Quarantined messages are removed permanently from the cloud infrastructure 30 days after the subscription has terminated.
Attachment Parking	Attachment Parking, when enabled, allows a customer to 'park' large attachments in inbound emails in our cloud infrastructure rather than deliver them directly to the user. The complete attachment is parked along with its associated data and the user can subsequently download these attachments.	Bandwidth efficiency & customer flexibility.	Emails with attachments to be parked are identified in the cloud data center that the customer MX record connects to. The parked attachment is retained in this cloud data center for download by the user.	During subscription term: - Parked attachments are retained in the cloud infrastructure for a customer configurable maximum period of 30 days unless they are downloaded by the user earlier after which they are removed permanently. After subscription term: - Parked attachments are removed permanently from the cloud infrastructure 30 days after the subscription has terminated.
Keep a Copy	Keep a Copy, when enabled, allows a copy of clean email messages to be retained for a period of 3 days so that they can be subsequently reported to	Efficacy improvements.	Keep a Copy mails are identified in the cloud data center that the customer MX record connects to. The Keep a Copy email is retained in	During subscription term: - Keep a Copy emails are retained in the cloud infrastructure for a period of 3 days after which they are removed permanently.

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
	Forcepoint, typically as spam.		this cloud data center for subsequent use.	After subscription term: - Keep a Copy emails are removed permanently from the cloud infrastructure 3 days after the subscription has terminated.
Standard Encryption	Standard Encryption, when enabled, allows customers to provide secure encrypted access to their sent emails. Rather than sent the original email, the recipient is sent an email which contains a link to the original email which is held within our infrastructure. To access the email, the recipient accesses the Forcepoint cloud infrastructure through a secure login.	Deliver messages securely.	Standard Encryption retains the original sent email in the cloud data center that the customer has configured for outbound emails. Standard Encryption retains the email in this cloud data center for subsequent access by the recipient.	During subscription term: - Standard Encryption emails are retained in the cloud infrastructure for a period of 30 days after which they are removed permanently. After subscription term: - Standard Encryption emails are removed permanently from the cloud infrastructure 30 days after the subscription has terminated

Add-on Modules

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
Advanced Malware Detection	Advanced Malware Detection receives files, which are to be analyzed for malware, from the Email Security Cloud product. Upon receiving the file, AMD conducts a behavioral analysis of the file to determine whether malware is contained in the file. Files uploaded to be analyzed by AMD may potentially contain sensitive information. The customer administrator is able to configure which file types are submitted to AMD.	The objective is to understand if the submitted file as a whole presents a malware risk and allow the customer policy to remove it.	Advanced Malware Detection stores the result of the malware analysis which is tied to the file hash generated by AMD. The submitted file is immediately deleted upon completion of the analysis. Analysis can take between 10 seconds to 5 minutes, depending on the size and type of the file being analyzed. The file is submitted to AMD via a secure encrypted channel (TLS encryption). The behavioral analysis capability of AMD is outsourced. Analysis takes place in two data centers, located in Los Angeles, United States and Amsterdam, Netherlands.	Advanced Malware Detection does not retain the submitted file. AMD retains the analysis results of a file indefinitely. Furthermore, if any malware code is found during analysis, the malware code (malware artefact) is kept indefinitely.
Image Analysis Module	The optional Image Anaylsis Module inspects images in email messages to determine whether they are pornographic or not.	Ensure users are protected from pornographic images.	Emails with image attachments deemed to be pornographic are identified in the cloud data centers that the customer MX record connects to. The quarantined message is retained in this cloud data centre for download by the user.	During subscription term: - Quarantined messages are retained in the cloud infrastructure for a customer configurable maximum period of 30 days unless they are downloaded by the user earlier after which they are removed permanently. After subscription term: - Quarantined messages are removed permanently from the cloud infrastructure 30 days after the subscription term has ended.
Email Encryption Module	This add-on (previously Advanced Encryption), when enabled, allows customers to provide secure encrypted access to their sent emails. The original email is encrypted using Voltage Securemail and delivered to the recipient. To access the email, the recipient creates a Voltage Securemail account and is then able to decrypt the content.	To provide the option to deliver email messages securely using encryption.	The Email Encryption Module does not retain the original sent email in the cloud data centers.	Advanced Encryption does not retain the original sent email.

Appendix A

TERMINOLOGY

Term	Explanation
Cloud data center	Forcepoint co-located, ISO27001 certified, Tier 4 data centers.
Cloud infrastructure	Components and services within cloud data centers.
Cloud portal	Web based portal access to Forcepoint cloud services.
Email Security Cloud	Forcepoint's cloud-based email protection product, which runs as a hosted service within Forcepoint's cloud data centers

Table 1: Cloud Portal Contacts Personal Data Attributes

Cloud portal contacts can contain the following personal data subject to configuration.

Attribute	Requirement
First Name	Optional
Last Name	Mandatory
User Name	Mandatory
Account (Employer)	Automatic
Contact Type	Mandatory
Job Title	Optional
Department	Optional
Contact Address	Optional
Post/Zip code	Optional
Country	Optional
Email address	Optional

Table 2: Directory Synchronization Data Personal Data Attributes

The following personal data 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: Email Policy Personal Data Attributes

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

Attribute	Requirement
Postmaster	Mandatory email address
Notifications & Annotations	Optional email address
Phishing Exceptions	Optional email address
Executable Exceptions	Optional email address
Message encryption	Optional email address
URL Sandbox Exceptions	Optional email address
Antispam Exceptions	Optional email address
Attachment Exceptions	Optional email address
Content Filter Exceptions	Optional email address

Table 4: Report Center Personal Data Attributes

The following information, which might potentially contain personal data, is available in Report Center.

Attribute
Envelope Sender
From: Address
Recipient Address
Sender Name
Subject
Sender IP
To: Address (INTERNAL HELD)

Table 5: Legacy Reporting Personal Data Attributes

The following information, which might potentially contain personal data, is available in Message Center.

Attribute
Envelope Sender
Recipient Address
Subject
Sender IP (Log)

Table 6: Audit Trail Personal Data Attributes

Personal data is not directly stored in this data set but is linked to the Cloud Portal Contacts records.

Attribute
Contact User Name (email address)
Account (via link to cloud portal contacts)

Table 7: Quarantine Items Personal Data Attributes

The following information, which might potentially contain personal data, is available in Quarantine Items.

Attribute
From: Address
Recipient Address
Subject
Email Body Content
Received Headers