FORCEPOINT
POWERED BY Raytheon

# Forcepoint Web Security Hybrid Management of Personal Data

# Forcepoint Web 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 Web Security Hybrid (formerly TRITON AP-WEB Hybrid)?” It is primarily intended for those involved in the procurement and privacy assessment of the Forcepoint Web Security Hybrid product.

Note: For Forcepoint Web Security Cloud deployments (formerly TRITON AP-WEB 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 Web 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 Web 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 | Is Anonymization Possible? | Storage, Flow & Protection | Retention |
|---|---|---|---|---|---|
| **Cloud Portal Contacts** (Tunneling only) | IMPORTANT: This applies only to customers who have requested the use of tunneling cloud connectivity methods.<br>If the customer has requested the use of tunneling connectivity functionality then Forcepoint will create a single cloud portal contact (login) based on information supplied by the customer and adhering to the rules in Table 1: Cloud Portal Contacts Personal Data Attributes below. | For the purpose of providing and controlling customer administrative access to tunneling connectivity functionality via the cloud portal. | Only partially. Some attributes in this data set have to be populated so that the cloud portal audit trail can function correctly to support security best practice. The remainder are optional and can therefore be left blank if required.<br><br>See Table 1: Cloud Portal Contacts Personal Data Attributes below for details. | Contact definitions are created in the cloud portal, stored centrally and then synchronized with three other cloud data centers for redundancy. | During subscription term:<br>- Contact definitions are held for the duration of the service subscription unless deleted by the Customer Administrator.<br>After subscription term:<br>- Contact definitions are permanently deleted from the Cloud Infrastructure 6 months after the Subscription Term has terminated. |
| **Directory Data** (Directory Sync) | Directory information is synchronized from the on-premise directory synchronization client to the cloud data centers.<br><br>See Table 2: Directory Synchronization Data below for details. | To allow end users to authenticate to the service and for the service to apply the correct security policy, | Only partially. Some attributes in this data set have to be populated so that the service authentication features can function correctly. The remainder are optional and can therefore be left blank if required.<br><br>See Table 2: Directory Synchronization Data Personal Data Attributes | Directory data is replicated to, and stored in, all cloud data centers on a schedule defined by the customer, but at least once per week. | During subscription term:<br>- Directory data is refreshed and replaced according to the directory synchronization schedule set by the customer administrator on the Directory Synchronization Client.<br>After subscription term:<br>- Directory data is permanently deleted from the cloud infrastructure 6 months after the Subscription Term has terminated. |
| **Policy** | Security/Acceptable Use Policy is defined by the customer administrator using the On-premise Manager. Policy data also includes SSL decryption categories and notification page definitions.<br><br>See Table 3: Policy Personal Data Attributes below for details. | To allow customer administrator defined security policy and acceptable use policy to be tailored to specific geographies, groups and/or individuals. | No. Personal data in this data set cannot be anonymized as this would prevent correct operation of the security policy.<br><br>See Table 3: Policy Personal Data Attributes below for details. | Policy definition data is created in the On-premise Manager, it is then synchronised with and stored in all of the cloud data centers. | During subscription term:<br>- Policy data is retained until the next policy version is synchronized at which point it is updated and replaced by the new policy version.<br>After subscription term:<br>- Policy 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 | Anonymization | Storage, Flow & Protection | Retention |
|---|---|---|---|---|---|
| **User Activity Logs** | User activity logs are created by the cloud infrastructure from the web browsing activity of cloud connected users. The logs contain details about web browsing , but not the web content.<br><br>See “Table 5: User Activity Log Download (sync) Log File Personal Data” below. | To provide granularity in the reporting system.<br>To provide details of each web transaction, to allow customers to understand how their users are accessing the web. | Yes. Data anonymization can be applied; see the Privacy Protection section below for details. | User activity log data is first created in the cloud data centers to which the customer connects. 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:<br>- User activity log files are retained in the cloud Infrastructure for 14 days, they are then removed permanently.<br>After subscription term:<br>- User activity logs are removed permanently from the cloud infrastructure 14 days after the Subscription Term has terminated. |
| **Endpoint Authentication Logs** | Endpoint authentication logs are created when an end user connects to the cloud infrastructure using a Forcepoint web endpoint. The authentication logs may contain user name (email address), IP address and workstation ID. | To provide traceability of web endpoint usage and to assist with troubleshooting connectivity issues. | No. Personal data in the endpoint authentication logs cannot be anonymized because this would contravene security best practice by muting the audit trail and because the log records do *not* tie a user to a particular behavior. | Endpoint authentication log data is first created in the cloud data centers to which the web endpoint user connects. The customer then copies the logs to their on-premise system on-demand via the log sync service when running the Hybrid Authentication Reports within 7 days of the log creation date. | During subscription term:<br>- Endpoint authentication log files are retained in the cloud Infrastructure for 90 days, they are then removed permanently.<br>After subscription term:<br>- Endpoint authentication log files are removed permanently from the cloud infrastructure 90 days after the Subscription Term has terminated. |
| **Cloud Portal Configuration Audit Trail** (Tunneling only) | IMPORTANT: This applies only to customers who have requested the use of tunneling cloud connectivity methods.<br>The cloud portal configuration audit trail records the administrative users (contacts) that made changes to the cloud portal configuration and details of those changes.<br><br>See Table 4: Audit Trail Personal Data Attributes below for details. | To provide traceability of cloud portal administrative activity. | No. Personal data in the Audit Trail cannot be anonymized as this would contravene security best practice.<br><br>See Table 4: Audit Trail Personal Data Attributes below for details. | Cloud portal audit trail records are stored in multiple cloud data centers selected automatically at service set-up based on the customer account’s country. 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:<br>- Cloud portal configuration audit trail data records older than 90 days are permanently deleted.<br>After subscription term:<br>- Cloud portal audit trail logs are de-coupled (orphaned) from the cloud portal contact records 6 months after the subscription term has terminated. This effectively anonymises the remaining cloud portal audit trail records as they can no longer be associated with a person or account. |

## Add-on Modules

| Data Set | What Data is Used? | Purpose | Anonymization | Storage, Flow & Protection | Retention |
|---|---|---|---|---|---|
| **Advanced Malware Detection** - (AMD based) | Advanced Malware Detection receives files, which are to be analyzed for malware, from the Web Security Hybrid product. Upon receiving the file, AMD conducts a behavioural analysis of the file to determine the whether malware is contained in the file.<br><br>Files uploaded to be analyzed by AMD may potentially contain sensitive information.<br><br>The customer administrator is able to configure which file types are submitted to AMD. | The sole objective is to understand if the submitted file as a whole presents a malware risk. | The results of the files are anonymized by generating a hash of the submitted file and associating the result of the analysis with the file hash. Upon completion of the analysis, the file and any of its contents are then immediately deleted | Advanced Malware Detection stores the result of the malware analysis which is tied to the file hash which is 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).<br><br>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. |
| **Cloud Application Control (CASB) add-on module** | After applying normal Web Security Hybrid processing, traffic identified by the customer administrator as requiring additional protection controls is forwarded to the Forcepoint CASB cloud infrastructure for further processing.<br><br>Please consult the 'Forcepoint CASB Management of Personal Data' document for further details. | | | | |

## Privacy Protection (Anonymization) Feature Operation

The Privacy Protection feature applies to Activity Logging defined above and according to Table 5 “Personal Data Attribute Cross Reference“ below.

| Area | Description | Anonymization Capability | Applicability |
|---|---|---|---|
| **Web Privacy** | Personal data can be anonymised in a granular fashion to help meet customer’s compliance needs.<br><br>User activity logs can be anonymised using two controls:<br><br>1) Preventing the logging of certain data attributes:<br>- IP addresses (Client IP)<br>- User names (User ID)<br><br>See Table 5: User Activity Log Download (sync) Log File Personal Data below.<br><br>2) Selective Category Logging allows the customer administrator to exclude logs records associated with selected URL categories from User Activity Logging. | When data is anonymised it is simply not stored, so it cannot be recovered.<br><br>Anonymization applies to both the on-premise reporting database and the cloud infrastructure used by cloud connected users. Data is anonymised in the cloud as log records are created, before being downloaded by the customer via the directory synchronization client. | Anonymization only affects data from the time at which it is enabled by the customer administrator; it is not applied retrospectively. |

# Appendix

## 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. |
| Cloud Portal | Web based portal used to access Forcepoint cloud services. |
| On-premise Manager | Forcepoint Web Security management console located on customer premises. |

### Table 1: Cloud Portal Contacts Personal Data Attributes

Note: This applies only to customers who have requested the use of tunneling cloud connectivity methods. Personal data in this data set cannot be anonymised as this would contravene security best practice by muting the cloud portal audit trail, however several items are optional.

| Attribute | Requirement |
|---|---|
| First Name | Mandatory |
| Last Name | Mandatory |
| User Name | Mandatory (same as email address) |
| Account (Employer) | Automatic |
| Contact Type | Mandatory |
| Job Title | Mandatory |
| Department | Optional |
| Contact Address | Optional |
| Post/Zip code | Optional |
| Country | Mandatory |
| Email address | Mandatory |
| Office Telephone | Mandatory |

### Table 2: Directory Synchronization Data Personal Data Attributes

Mandatory personal data in this data set cannot be anonymised as this would prevent the authentication features from functioning.

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

### Table 3: Policy Personal Data Attributes

Personal data in this data set cannot be anonymized as this would prevent correct operation of the security policy.

| Attribute | Requirement |
|---|---|
| Email Address | Mandatory |

### Table 4: Audit Trail Personal Data Attributes

IMPORTANT: This section applies only to customers who have requested use of tunneling cloud connectivity capabilities.

Personal data is not directly stored in this data set but is linked to cloud portal contact records. Linked personal data in this data set cannot be anonymized as this would contravene security best practices by muting the cloud portal audit trail.

| Attribute |
|---|
| User Name (via link to cloud portal contacts) |
| Account (via link to cloud portal contacts) |

### Table 5: User Activity Log Download (sync) Log File Personal Data

Web Activity log data that is downloaded from the Cloud Infrastructure by the customer's on-premise system may contain the following personal data. Please read this section in conjunction with "User Activity Logs" and "Privacy Protection" sections above.

| Field | Anonymizable? | Description |
|---|---|---|
| User ID | Yes | The user's NTLM or LDAP address. |
| Client IP | Yes | The client's (external) Internet IP address. |
| Date and Time | | The time that the request occurred on the proxy recorded in Unix epoch time. |
| Account ID | | The internal hosted customer identifier. |
| Request Count | | The number of requests to a given site. |
| Request Size | | Size in bytes of the complete request. |
| Response Size | | Size in bytes of the complete response. |
| Protocol | | The protocol used in the request (HTTP, HTTPS or FTP only). |
| Destination port | | The destination port used for the request. |
| Destination IP | | The requested IP address. |
| URI | | The exact page that the user requested (The Full URL). |
| Method | | Method (GET, POST, PUT…). |
| Content Type | | Content-Type header field. Value of first "content-type" header in response. |
| Network Direction | | Direction where analytic scanning occurred. |
| Policy Names | | Policy name, will be blank if page is NOT blocked. |
| File Name | | String that holds the file name extracted from URL. |
| True File Type Code | | Hybrid True File Type code. |
| Category Reason Code | | Category Reason code. |