FORCEPOINT
POWERED BY Raytheon

Forcepoint Web Security Cloud
Management of Personal Data

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

Note: For Forcepoint Web Security Hybrid deployments (formerly TRITON AP-WEB 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 Web 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 Web 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 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	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 below for details.	For the purpose of providing and controlling customer administrative access to the service 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 practices. The remainder are optional and can therefore be left blank if required. See Table 1: Cloud Portal Contacts Personal Data Attributes below for details.	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 term has terminated.
Directory Data *(Directory Sync)*	Directory information is synchronized from the on-premises Directory Synchronization Client to the cloud data centers. 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. See Table 2: Directory Synchronization Data Personal Data Attributes	Directory data is replicated to, and stored in all cloud data centers.	During subscription term: - Directory data is refreshed and replaced according to the directory synchronization schedule set by the customer administrator via the Directory Synchronization Client. After subscription term: - 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 cloud portal. Policy data also includes SSL decryption categories and notification page definitions. Customer entered Data Security classifiers could potentially contain personal data. See Table 3: Policy Personal Data Attributes below for details.	To allow security policies and acceptable use policies defined by customer administrators 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. See Table 3: Policy Personal Data Attributes below for details.	Policy definition data is created in the cloud portal, stored centrally and then synchronized with all of the cloud data centers.	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 term has terminated.

Activity Logging

Data Set	What Data is Used?	Purpose	Anonymization	Storage, Flow & Protection	Retention
User Activity Logs *(Includes Web Activity, Authentication, and Endpoint Auditing.)*	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, authentication, and network activity, but not the web content. See Table 5: Personal Data Attribute Cross Ref - Data Log Records for details.	To provide granularity in the reporting system. 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. See Table 5: Personal Data Attribute Cross Ref - Data Log Records for details.	User activity log data is first created in the cloud data centers that the end users connect to. It is then fed back to the cloud data centers set as the account's data storage locations. Storage locations are configured by the customer administrator at service set-up. These can subsequently be changed subject to written request from the customer.	During subscription term: - As standard user activity log file data records older than 90 days are permanently deleted. - At subscriber's option, user activity log files data records 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 term has terminated.
Data Security Event Logs	The Data Security feature, when enabled by the customer administrator, captures event information that may trigger compliance rules such as HIPAA, PCI, etc. Such event information may contain data such as credit card number, sensitive text phrases, etc. Personal data may form part of the event capture.	To provide details that will assist with event remediation.	Yes - Data anonymization can be applied; see the Privacy Protection section below for details. **Note**: By default, highly sensitive data types, such as credit card and social security numbers, are automatically stored in hashed format. For example, a credit card with CNN 4111-1111-1111-1111 will be stored as 4111-xxxx-xxxx-1111.	Data security event log data is first created in the cloud data center that the end user connects to. It is then fed back to the cloud data centers set as the account's data storage locations. Storage locations are configured by the customer administrator at service set-up. These can subsequently be changed subject to written request from the customer. Data security event log data is stored at the same locations as User Activity Logs (see above).	See User Activity Logs above.
I Series Appliance	User activity logs are created by the I Series appliance from the web browsing activity of users protected by the appliance. The logs contain details about web browsing,	To provide granularity in the reporting system. To provide details of each web transaction, to allow customers to understand how their users are	Yes. Data anonymization can be applied; see the Privacy Protection section below for details.	User activity and protocol log data is encrypted in the cloud infrastructure and then processed in the same way as regular User Activity Logs (see above).	See User Activity Logs above.

Data Set	What Data is Used?	Purpose	Anonymization	Storage, Flow & Protection	Retention
	authentication, and network activity but not the web content. See Table 5: Personal Data Attribute Cross Ref - Data Log Records “Web Activity” column below. Network protocol logs can also be created by the I Series appliance for traffic passing through it. These logs contain details about network traffic but not the traffic content. See Table 5: Personal Data Attribute Cross Ref - Data Log Records for details “I Series” column below.	accessing the web.			
Full Traffic Logging	The Full Traffic Logging (FTL) feature, when enabled by the customer administrator, creates a feed of user activity log record data. This contains selected details of web browsing activity but not the web content.	Optionally used by the customer administrator to transfer web activity log data records to customer’s Security Information and Event Management (SIEM) systems and/or log facilities.	No. Data anonymization features are not supported in this data set.	User activity log record data is extracted according to FTL policy set by the customer administrator for selected or all security policies. FTL log files reside in the cloud data centers selected by the customer administrator for the account at service set-up. The customer pulls copies of the FTL logs to their on-premise system using the sync service on a schedule of their choosing, but within 14 days of the log creation date.	During subscription term: - New FTL log file entries are retained in the cloud web infrastructure for a rolling 14 day period before being automatically aged out, they are then permanently deleted. After subscription term: - FTL logs age out and are permanently deleted from the cloud web Infrastructure 14 days after the subscription term has terminated.
SIEM Integration *(beta only)*	SIEM integration is an evolution of the former Full Traffic Logging feature. When enabled by customer administrator, the SIEM integration feature can be used by the customer administrator 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.	When enabled by the customer administrator, data anonymization features are supported. The customer administrator is also at liberty to control which data attributes are included in the SIEM integration data records. See Table 5: Personal Data	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	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

Data Set	What Data is Used?	Purpose	Anonymization	Storage, Flow & Protection	Retention
	(Web Activity or Data Security). See Table 5: Personal Data Attribute Cross Ref - Data Log Records for details.		Attribute Cross Ref - Data Log Records for details.	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.	permanently from the cloud web infrastructure 14 days after the subscription term has terminated.
Cloud Portal Configuration 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 4: Audit Trail Personal Data Attributes below for details.	To provide traceability of cloud portal administrator activity.	No. Personal data in the audit trail cannot be anonymized as this would contravene security best practice.	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 cloud portal configuration audit trail data records older than 90 days are permanently deleted. - At subscriber's option, cloud portal configuration audit trail data records 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: - 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 anonymizes 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 Cloud product. Upon receiving the file, AMD conducts a behavioural 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 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 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.
Cloud Application Control (CASB) add-on module	After applying normal Web Security Cloud processing, cloud application traffic identified by the customer administrator as requiring additional protection is forwarded to the Forcepoint CASB cloud infrastructure for further processing. Please consult the 'Personal Data Management for Forcepoint CASB' 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	The Privacy Protection feature allows personally identifiable information (personal data) to be anonymized in data log records. Anonymization is granular so the customer only needs to anonymize those personal data items and policies required to meet their compliance scenario, e.g. compliance requirements vary by country and can be often be met by applying anonymization to only a selection of policies. Each personal data attribute can be individually controlled by the customer administrator. When the anonymization feature is enabled, the default is to anonymize all personal data attributes: - Connection IP / Connection Name - IMEI Number - Source IP - Use Name - Workstation In addition, the customer administrator can choose to preserve personal data for security threat related events to assist with troubleshooting and remediation. See Table 5: Personal Data Attribute Cross Ref in the Appendix below for details.	Enabling anonymization for a personal data attribute means that the personal data attribute is anonymised in associated service data log records where this information would tie a user to a specific behavior. When data is anonymized it is simply not stored, so it cannot be recovered. See Table 5: Personal Data Attribute Cross Ref in the Appendix below for details.	Anonymization only affects data from the time at which it is enabled by the customer administrator; it is not applied retrospectively.
Data Security Incident Data Privacy	The customer administrator can choose whether or not to capture, store, display and report on data that triggered data security incidents (e.g., credit card numbers, sensitive text phrases, etc.). This helps to guard private data and/or comply with a company security policy.	Enabling anonymization for data security incident data means that this data is anonymized in associated service data stores. See Table 5: Personal Data Attribute Cross Ref in the Appendix below for details. **Note**: Highly sensitive data types, such as credit card and social security numbers, are automatically stored in hashed format regardless of Privacy Protection settings. For example, a credit card with CNN 4111-1111-1111-1111 will be stored as 4111-xxxx-xxxx-1111.	Anonymization only applies to data from the time the anonymization feature is activated. It cannot be applied retrospectively.

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.
Cloud portal	Web-based portal used to access Forcepoint cloud services.
Web Security Cloud	Forcepoint's cloud-based web protection product, which runs as a hosted service within Forcepoint's cloud data centers.

Table 1: Cloud Portal Contacts Personal Data Attributes

Personal data in this data set cannot be anonymized as this would contravene security best practices by muting the cloud portal audit trail, however several items are optional.

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
Office Telephone	Optional

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

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: Personal Data Attribute Cross Ref - Data Log Records

Full details of the available reporting attributes can be found in the cloud portal context-sensitive help menus.

Personal Data Attribute	User Activity Logs			Data Security	I Series	FTL	SIEM	Cloud Portal	
	User Activity Logs (WEB schema)	Authentication (AUTH schema)	Web Endpoint Auditing	Data Security Event Logs (DLP schema)	Network Protocol[3] (PROT schema)	Full Traffic Logging logs	SIEM Integration logs[4]	Cloud Portal Config Audit Trail	Cloud Portal Contacts
Connection IP[1]	Yes	-	-	-	-	No	Yes	-	-
Connection Name[1]	Yes	-	-	-	-	No	Yes	-	-
IMEI Number (mobile)[2]	Yes	-	-	-	-	No	Yes	-	-
Source IP	Yes	-	-	Yes	Yes	No	Yes	-	-
User / User Name	Yes	NA	NA	Yes	Yes	No	Yes	NA	NA
Workstation	Yes	NA	NA	-	-	No	Yes	-	-
Data Security Trigger Event Values	-	-	-	Yes	-	NA	Yes	-	-

Yes = Personal data attribute can be anonymized in this schema or file.

No = Personal data attribute cannot be anonymized in this schema or file.

NA = Attribute exists in this schema but anonymization is not applicable as it does not tie a user to specific behavior.

"-" = Attribute does not exist in this schema.

[1] *Selecting "Connection IP" causes "Connection Name" to also be anonymized.*

[2] *Applies when Mobile module is used.*

[3] *Applicable to I Series appliance only.*

[4] *SIEM feed log record content is customisable by the customer administrator and adheres to data anonymization configuration.*