FORCEPOINT
POWERED BY Raytheon

Forcepoint CASB
Management of Personal Data

Forcepoint CASB – 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 CASB?”. It is primarily intended for those involved in the procurement and privacy assessment of the Forcepoint CASB product.

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 CASB 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 CASB’s cloud 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
CASB Portal Administrators	CASB Administrators are created by the customer administrator. An initial administrator is created as part of service provisioning, thereafter the customer is free to create and manage new administrators as required. See Table 1: CASB Administrator Personal Data Attributes below for details.	For the purpose of providing administrative access to the CASB service via the CASB portal or CASB API.	CASB Administrator details are created in the CASB portal & stored (encrypted) in the configuration DB.	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 cloud infrastructure 6 months after the subscription term has terminated.
Directory Data *(User Data)*	Directory information is synchronized from the on-premise Active Directory through the AD Agent to the CASB Service. Another option is manual import through CSV file. See Table 2: Directory Synchronization Data below for details.	To allow the service to provide the correct security policy for the relevant users. To allow multi factor authentication for the users. To allow user level notifications.	Directory data is synced to the CASB configuration DB, and to all customer related Gateways and Evaluators.	During subscription term: - Directory sync data is refreshed and replaced according to the directory synchronization schedule set by the customer, or the manual file import. - Deleting the AD entity will remove the data from these locations within 10 minutes. After subscription term: If not manually deleted (see above), directory data is permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.
Policy *(Custom Policy, Anomaly Detection)*	CASB custom / quick policies are defined by the customer administrator using the CASB Portal. Policy data may include personal data such as user name or business unit. See Table 3: Policy Personal Data Attributes below for details.	To allow customer admin defined security policy to be tailored to specific geographies, groups and/or individuals.	Policy data is created in the CASB Portal, stored in the configuration DB and then synchronized to all customer related Gateways and Evaluators.	During subscription term: - Policy data is retained until the policy is deleted or modified by the customer administrator. 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	Storage, Flow & Protection	Retention
User Activity Logs *(Includes Realtime monitoring Audit log & Dashboard, Service provider log Audit log & Dashboard, Audit and Protect dashboard, Incidents, All detailed reports)*	User activity logs are created by the CASB infrastructure based on the activity of cloud service connected users. The information is collected from real-time activities when CASB is in inline mode, and from service provider audit logs when in API mode. The logs contain details about the user location, device, activity (action), service modules accessed, service details, accessed files (path/name), as well as user property enrichment from Active Directory. See Table 1: CASB Administrator Personal Data Attributes below for details.	To provide granularity in the reporting system.	User activity log data is first created in the gateway that the end users connect to, or in the Evaluator getting the service provider audit logs. It is then sent to the CASB big data DB in the cluster selected by the customer (US / EU). Storage locations are set by Forcepoint Operations based on customer request. These can subsequently be changed subject to written request from the customer, however data and configuration migration is not supported.	During Subscription term: - Audit logs and dashboard data retention is for 30 days. - Reports and export options such as SIEM keep data for 6 months. After subscription term: - User Activity Log records are permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.
Data Leak Prevention Event Logs *(Includes Realtime monitoring Audit log & Dashboard, Service provider log Audit log & Dashboard, Audit and Protect dashboard, Incidents, All detailed reports)*	DLP inspection can be set as part of the CASB standalone functionality or as part of the Forcepoint DLP Cloud Apps module. When enabled by the customer administrator, captures event information that may trigger compliance rules such as HIPAA, PCI, etc. The collected information includes data classifier, rule, and policy names, but not the actual detected data.	Personal Data may form part of the event capture when a DLP Security rule is triggered.	DLP data is first created as part of the event in the CASB Gateway that the end users connect to, or in the Evaluator getting the service provider audit logs. It is then sent to the CASB big data DB in the cluster selected by the customer (US / EU). Storage locations are set by Forcepoint Operations based on customer request. These can subsequently be changed subject to written request from the customer, however data and configuration migration is not supported.	During subscription term: - Audit logs and dashboard data retention is for 30 days. - Reports and export options such as SIEM keep data for 6 months. After subscription term: - Data leak prevention event records are permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.
Accounts (Users)	The accounts reports share summary of the key information collected over each user. It includes private data alongside the user risk, summary of the user activity and incidents, and statistics about the user profile and behaviour.	Personal data is displayed to help identify the employee and understand the risk they are posing	Accounts data is collected from multiple sources mentioned in this report. Data is collected through Active Directory sync, user activity logs and data classification. The data is stored in the CASB big data DB in the cluster selected by the customer (US / EU). Storage locations are set by Forcepoint Operations based on customer request. These can subsequently be changed subject to written request from the customer, however data and configuration migration is not supported.	During subscription term: - Account data is retained for 6 months. After subscription term: - Accounts records are permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
Data Classification	Data classification is DLP based classification of data at rest stored in cloud storages. When enabled by the customer administrator, scans and captures files that may trigger compliance rules such as HIPAA, PCI, etc. The collected information includes data classifier, rule, and policy names, but not the actual detected data.	The correlation to the user is reporting on content owner and users/groups the content is shared with.	File classification is first created as part of the CASB Scanner event in the CASB cluster selected by the customer (US/EU). The data is then transferred to the big data DB. Storage locations are set by Forcepoint Operations based on customer request. These can subsequently be changed subject to written request from the customer, however data and configuration migration is not supported.	During subscription term: - Data classification info is removed when the sensitive content - DLP breach - is resolved. - Customers may control that by adjusting the policy or by removing the sensitive files. After subscription term: - Data classification information is permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.
Data Export *(SIEM & CASB API Integration)*	SIEM & API Integration allow customers to export data from the CASB service to their own SIEM/SOC systems or for any other purpose. The exported data includes the data described above as part of the user activity log.	See User Activity Logs above.	SIEM Integration records are extracted from the CASB big data DB by the SIEM tool or leveraging the CASB API, thus transferred to a customer controlled location. The data is extracted based on permissions assigned with the administrator setting up the export. All event and user related data residing in the DB can be exported.	Data transferred through the SIEM tool is stored in a customer controlled location and is retained based on the customer's retention policy. Forcepoint does not retain this data. Forcepoint recommends that customers follow their company data retention policies and industry best practices for GDPR-relevant data.
CASB Administrator Activity Auditing	The CASB Administrator Activity Auditing captures every admin activity in the CASB portal. This information is similar to Event activity log, this time tracked for the administrators activity in the CASB portal.	See User Activity Log above, (Administrators are regarded as users).	CASB Administrator activity auditing records are stored in the CASB Big data DB in the cluster selected by the customer (US / EU).	During subscription term: - Data is kept for 6 months. After subscription term: - User Activity Log records are permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated.
Advanced Malware Detection	Advanced Malware Detection receives files, which are to be analyzed for malware, from the CASB 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.	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 behavioural 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.

Data Set	What Data is Used?	Purpose	Storage, Flow & Protection	Retention
Shadow-IT Discovery	Shadow-IT provides a list of cloud services accessed by the users alongside the risk factors for this service, the IPs and users accessing each of the services and traffic volume.	Provide granular info on the users leveraging each service.	Shadow-IT data is first detected by the CASB Discovery tool run by the customer in their controlled environment over traffic logs exported from the customer firewall / web proxy. The data is processed by the tool. The analysis results (metadata) are exported locally into file and uploaded (optional) to the CASB portal where they are stored in the big data DB in the cluster selected by the customer (US / EU).	During subscription term: - Shadow IT info is kept for 6 months. After subscription term: - Shadow IT information is permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated
Endpoints	Devices used by each user are tracked with details such as device type, OS, user agent, and activity times.	Profile user behaviour with regards to used devices and allow both access control and anomalous behaviour protection as part of the CASB policy.	Endpoint data is first created as part of the event in the CASB Gateway that the end users connect to, or in the Evaluator getting the Service Provider Audit logs. It is then sent to the CASB big data DB in the cluster selected by the customer (US / EU). Storage locations are set by Forcepoint Operations based on customer request. These can subsequently be changed subject to written request from the customer, however data and configuration migration is not supported.	During subscription term: - Endpoints data is kept for 6 months. After subscription term: - Endpoints data is permanently deleted from the cloud infrastructure 6 months after the subscription term has terminated

Appendix A

TERMINOLOGY

Term	Explanation
CASB Cluster & Infrastructure	Forcepoint CASB cluster hosted over Amazon AWS infrastructure, leveraging multiple availability zones. The CASB portal and the CASB infrastructure are hosted in Two areas: United States (North California) & Europe (Frankfurt). Customers may select the cluster they wish to maintain their data (US/EU).
CASB Evaluators	CASB Evaluators are the CASB analysis units when operating in API mode. The Evaluators are part of the CASB infrastructure.
CASB Gateways	CASB Gateways are the CASB proxies protecting the customer assets when in inline mode. Gateways can be hosted at any of the AWS regions and the customer may select the region(s)
CASB Portal	Web based portal access to the CASB service allowing management and control for the customer administrator.

Table 1: CASB Administrator Personal Data Attributes

Personal data in this data set cannot be anonymised as this would contravene security best practice by muting the cloud portal audit trail.

Attribute	Requirement
Email (acting as portal username)	Mandatory
Full Name	Optional
Phone number	Optional
Time zone	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. Optional fields may be excluded, however doing so will limit some of the product functionality.

Attributes	Requirement
sAMAccountName	Mandatory
Account	Mandatory
First Name	Optional
Last Name	Optional
Account Email Address	Mandatory
Account Phone	Optional
Title	Optional
Business Unit	Optional
3 custom fields can be adjusted to retrieve more information from the AD	Optional
DN	Mandatory
Account Status	Optional
User Photo	Optional

Table 3: Policy Personal Data Attributes

Personal data in this data set cannot be anonymised as this would prevent correct operation of the security policy. Optional items may be excluded, however doing so will limit some of the product functionality.

Attribute	Requirement
Login Name	Mandatory
Account	Mandatory
Full Name	Optional
Business Unit	Optional
3 custom fields can be adjusted to retrieve more information from the AD	Optional
OS Username	Optional
User location	Mandatory

Table 4: User Activity Log Personal Data Attribute Cross Reference - Data Log Records

Full details of the available reporting attributes can be found in the CASB administrator Guide.

Personal Data Attribute (Personally Identifiable Information)	User Activity Log	DLP Events	Data Export	Accounts	Data Classification	Endpoints	Shadow-IT
Account	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login name	Yes	Yes	Yes	Yes		Yes	Yes
Full name	Yes	Yes	Yes	Yes	Yes	Yes	
Title	Yes	Yes	Yes	Yes	Yes	Yes	
Business unit	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Source IP	Yes	Yes	Yes	Yes			Yes
Location	Yes	Yes	Yes	Yes		Yes	
Record (may contain user name)	Yes	Yes	Yes				
Data types		Yes	Yes		Yes		
Data policies		Yes	Yes		Yes		
OS Username	Yes	Yes	Yes			Yes	
Endpoint type	Yes	Yes	Yes	Yes		Yes	
Endpoint OS	Yes	Yes	Yes	Yes		Yes	
File owner				Yes	Yes		
File shared with	Yes	Yes	Yes				