
Forcepoint
Advanced Malware Detection and Protection (AMDP) 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 Forcepoint Advanced Malware Detection and Protection (AMDP)?" It is primarily intended for those involved in the procurement and privacy assessment of Forcepoint Advanced Malware Detection and Protection (AMDP).

Privacy Laws

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, along with other applicable data privacy laws, guide the principles that are incorporated in 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.

Forcepoint Advanced Malware Detection and Protection (AMDP) is designed to comply with applicable data privacy principles, including those contained in GDPR. Consistent with these principles, Forcepoint's customers are considered to be the sole data controller. Forcepoint is the data processor with respect to customer data transferred through or stored in Forcepoint Advanced Malware Detection and Protection (AMDP)

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 protect data held within the Forcepoint product, including personal data. Full details on Forcepoint's privacy policy and processes can be found at: https://www.forcepoint.com/legal/forcepoint-trust-hub. https://www.forcepoint.com/

License Cache

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Customer license information such as websense ID, Proof of License, subcheck ID, sandbox provider licensed for use and license expiration time.	IDs fetched from Salesforce are tenant specific and not user specific. An ID cannot be used to identify an individual end user, it is only useful for associating a customer with their account in Salesforce. All IDs are stored in AMDP's local database (Redis).	IDs and their associated license details from Salesforce are used to validate requests sent to AMDP and determine the sandbox provider to route them to.	The IDs cannot be used to identify any personal data.	The database is hosted on AMDP servers located in Forcepoint datacenters. Server access (and hence database access) is controlled by user authentication, and authorized users are limited to authorized Forcepoint employees.	Data stored in the database is retained while it exists in Salesforce. Once data is deleted from Salesforce, it is removed from the database as well. Data in Salesforce is managed by Sales.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	This data is not directly accessible by the end user and can only be requested via a Forcepoint representative.
SAR - Correction/Rectification	Changes to the data can be requested via a Forcepoint representative and implemented in Salesforce. Any changes to the data made in Salesforce will be reflected in the AMDP's local database within 12 hours.
SAR - Right to be Forgotten	Data removal can be requested via a Forcepoint representative and implemented in Salesforce. Entries deleted from Salesforce will be removed from AMDP's local database within 12 hours.
Data Storage / Localization	Local database is in the AMDP server closest to the end client's location (which is a Forcepoint product) as determined by Geo DNS (Domain Name Service). AMDP servers are deployed in Paris, Heathrow, and San Jose. This database is managed by AMDP and is separate from any database managed by the Sandbox Providers.

License alerts

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Expired license usage count associated with a tenant specific ID.	AMDP API (Application Programming Interfaces) usage count for expired licenses contains no personal data. The licenses are identified with an ID which is tenant specific, but not user specific. This ID is retrieved from Salesforce and is only useful for associating a customer with their Salesforce information.	This information is used to keep track of expired license usage and file submission counts. Instead of rejecting requests from customers with expired licenses, an email alert will be sent to the relevant Forcepoint parties (sales) so they can facilitate license renewal for these customers.	Tenant IDs stored in the database and sent in the alerts are not personal data and cannot be used to identify a user.	The database is hosted on AMDP servers located in Forcepoint datacenters. Server access (and hence database access) is controlled by user authentication, and users are limited to authorized Forcepoint employees. Communication with Grafana cloud (which will store and render AMDP's license cache) is over TLS. The alert emails will only be sent to authorized Forcepoint employees.	Data in Grafana will be retained for a year. Expired license usage alerts will be emailed as needed to a Forcepoint account and email retention will be determined by Forcepoint's email retention policy. Usage counts in AMDP's database will be reset monthly. IDs are stored in the database until the customer information exists in Salesforce.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	This information is available in the emails sent to the Forcepoint service account and can be made available on request to a Forcepoint representative. The user cannot access this information directly.
SAR - Correction/Rectification	Monthly usage counts in the database can be corrected on request.
SAR - Right to be Forgotten	Monthly usage counts in the database can be deleted on request.
Data Storage / Localization	The local database is in the AMDP server closest to the end client's location (which is a Forcepoint product) as determined by Geo DNS. AMDP servers are deployed in Paris, Heathrow, and San Jose.

File Contents

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Files submitted by customers for analysis. If using AMDP with Forcepoint Email Gateway, files sent to AMDP would be email attachments. If using AMDP with Forcepoint Cloud Web Security, files sent to AMDP could be any files downloaded from a browser.	Files are owned by the end users and could contain personal information. In the case of email, attachments are sent to AMDP (not email text). Once AMDP is enabled for a Forcepoint product - any files that pass through the product are sent to AMDP for analysis (barring any rules on the product itself that deem a file not suitable for scanning). An end user would not be able to choose which files go to AMDP for scanning.	Files uploaded to AMDP are stored on disk temporarily before being sent to the sandbox provider (Recorded Future) for analysis.	AMDP will retain a hash of the file submitted for analysis to uniquely identify a file. The hash cannot be used to reconstruct or identify the contents of a file.	The database is hosted on AMDP servers located in Forcepoint datacenters. Server access (and hence database access) is controlled by user authentication, and authorized users are limited to authorized Forcepoint employees. Recorded Future's database is separately hosted and maintained.	Files uploaded to AMDP are stored in tmpfs for 30 minutes before being deleted, and after a hash of the file is created and stored in AMDP's local database (Redis). Files sent to Recorded Future for analysis are kept in their environment for 40 days for file hash analysis verification purposes.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	An authorized Forcepoint employee with access to the AMDP servers can manually provide access to the files on request.
SAR - Correction/Rectification	Due to the nature of scanning and the temporary storage of files, uploading a new file with the corrected information is the path to correct/rectify information.
SAR - Right to be Forgotten	A request should be submitted to an authorized Forcepoint employee that can manually delete or request a deletion by Recorded Future.
Data Storage / Localization	Files are stored in the AMDP server closest to the end client's location (which is a Forcepoint product) as determined by Geo DNS. AMDP servers are currently deployed in Paris, Heathrow, and San Jose. Files are also stored on Recorded Future servers which are deployed in Netherlands and the United States.

File Hash Cache

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Hash (SHA-1, SHA-256 or SHA-512) of submitted file.	No personal data is identifiable using the file hash.	The local cache of file hashes is used to determine if a file has been previously uploaded to a sandbox provider and to associate the files present in an archive with the archive file.	File contents are not stored locally on Forcepoint servers, only hashes. It is not possible to reconstruct file contents from the hash.	The database is hosted on AMDP servers located in Forcepoint datacenters. Server access (and hence database access) is controlled by user authentication, and authorized users are limited to authorized Forcepoint employees.	Hashes in the database are automatically deleted after 2 hours.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Hashes stored in the database are not directly accessible by an end user but can be retrieved on request to a Forcepoint representative
SAR - Correction/Rectification	Hashes in the database directly correlate to the files submitted for analysis. While these hashes can be changed on request to a Forcepoint representative, submitting a new file is the solution to this request.
SAR - Right to be Forgotten	Hashes in the database are automatically deleted after 2 hours.
Data Storage / Localization	The local database is in the AMDP server closest to the end client's location (which is a Forcepoint product) as determined by Geo DNS. AMDP servers are deployed in Paris, Heathrow, and San Jose.

Logs

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
AMDP operational information such as incoming requests and associated processing information.	Logs should not contain any personal information, with the notable exception being filenames, which are at the discretion of the user and could contain personal data.	Logs are used to track file scan progression in AMDP and troubleshoot issues.	No pseudonymization in logs files.	Log files are stored on AMDP servers located in Forcepoint datacenters. Server access is controlled by user authentication, and authorized users are limited to authorized Forcepoint employees. Access to Forcepoint's Grafana cloud is controlled by user authentication, and only authorized Forcepoint employees are allowed access to this data.	Log files are retained for a maximum of 30 days on the AMDP server and Grafana cloud.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Logs are not accessible by the end user but can be requested from a Forcepoint representative.
SAR - Correction/Rectification	Since there is no personal data in the logs, this category does not apply.
SAR - Right to be Forgotten	Since there is no personal data in the logs, this category does not apply.
Data Storage / Localization	Logs are in the AMDP server closest to the end client's location (which is a Forcepoint product) as determined by Geo DNS. AMDP servers are deployed in Paris, Heathrow, and San Jose.

AMDP results queue

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
File scan results including file hash and its associated score.	No personal data is identifiable using the file hash.	The result queue is used to publish results of a file scan operation to Forcepoint X-labs for further processing. Forcepoint X-Labs uses this data to build out an internal database of known malicious files that is used by other Forcepoint products. Forcepoint X-Labs performs some validation of its own on the file results retrieved from this queue.	Only a hash of the file submitted for analysis will be published to the results queue, and not the file itself. The hash cannot be used to reconstruct or identify the contents of a file.	The queue is hosted on AMDP servers located in Forcepoint datacenters. Server access (and hence queue access) is controlled by user authentication, and authorized users are limited to authorized Forcepoint employees.	Data stays in the queue until it is read by a member of Forcepoint X-Labs, and the relevant corporate retention policy controls how long this data is kept.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Data published to the queue is not directly accessible by end users, but file scan reports and results are via the portal email for cloud web and cloud email customers. Reports contain additional details about the scan results.
SAR - Correction/Rectification	Since there is no personal data in the results queue, this category does not apply
SAR - Right to be Forgotten	Since there is no personal data in the results queue, this category does not apply.
Data Storage / Localization	The queue is in the AMDP server closest to the end client's location (which is a Forcepoint product) as determined by Geo DNS. AMDP servers are deployed in Paris, Heathrow, and San Jose.

Appendix A

TERMINOLOGY

Term	Explanation
Proof of License	Customer license identifier used by NGFW (Next Generation Firewall) (always hashed when stored on the AMDP server in its database or logs).
Rabbitmq	Message queue used to publish file scan results from AMDP to Forcepoint X-Labs.
Subcheck ID	Customer license identifier (always hashed when stored on the AMDP server in its database or logs).
Tmpfs	Temporary file system which stores data in volatile memory.
Websense ID	Customer identifier used in Salesforce. Useful for associating a customer with their Salesforce account.